Part No. 553-3001-230
August 2005

4401 Great America Parkway
Santa Clara, CA 95054

Optivity Telephony Manager Installation and Configuration

NORTEL >THIS IS THE WAY >THIS IS NORTEL™

Copyright © 2005 Nortel Networks Limited

Restricted rights legend

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

This product includes the following software:

The Purdue Compiler Construction Tool Set, written by Russell Quong June 30, 1995. Adapted by Terence Parr to ANTLR stuff. Parr Research Corporation with Purdue University and AHPCRC, University of Minnesota, 1989-1995.

SNMP Development Kit,written by James R. Davin, Advanced Network Architecture group, M.I.T Laboratory for Computer Science 45 Technology Square Cambridge, MA 02139 Copyright 1988, 1989 Massachusetts Institute of Technology. Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of M.I.T. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

SAX Parser for XML from Apache, Version 1.1 for SAX (Simple API for XML). Copyright (c) 1999-2000 The Apache Software Foundation (http://www.apache.org/). All rights reserved.

W3C DOM implementation for Java: Copyright 2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. http://www.w3.org/Consortium/Legal/

Cryptix MD5 (RFC 1321) and SHA-1 (NIST FIPS 180-1) message digest algorithms: Copyright (c) 1997 Systemics Ltd on behalf of the Cryptix Development Team.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. Optivity* Telephony Manager software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying Optivity Telephony Manager software or installing the hardware unit with pre-enabled Optivity Telephony Manager software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date the Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Revision history

August 2005

Standard 3.00. This document is up-issued to support Communication Server 1000 Release 4.5.

September 2004

Standard 2.00. This document is up-issued to up-issued for Communication Server 1000 Release 4.0.

October 2003

Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: Installing and Configuring Optivity Telephony Manager (553-3001-230).

Contents

Tables

Figures

About this document

Subject

Optivity Telephony Manager (OTM) is designed for managers of telecommunications equipment and authorized Nortel* distributors. OTM provides a single point of access for management of Nortel systems. OTM uses internet protocol (IP) technology to target:

- single point of connectivity to systems and related devices
- data collection for traffic and billing records
- collection, processing, distribution, and notification for alarms and events
- data entry and propagation (employee names and telephone numbers shared in multiple databases)
- Windows® and web-based management applications

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication server 1000 Release 4.0 software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support** on the Nortel home page:

http://www.nortel.com/

Applicable systems

This document applies to the following systems:

- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 61C CP PII
- Meridian 1 PBX 81
- Meridian 1 PBX 81C
- Meridian 1 PBX 81C CP PII
- Communication server 1000S (CS 1000S)

- Communication server 1000M Chassis (CS 1000M Chassis)
- Communication server 1000M Cabinet (CS 1000M Cabinet)
- Communication server 1000M Half Group (CS 1000M HG)
- Communication server 1000M Single Group (CS 1000M SG)
- Communication server 1000M Multi Group (CS 1000M MG)
- Communication server 1000E (CS 1000E)

  Note: When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 4.0 software and configured to include a Signaling server, they become CS 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a CS 1000M system.

Table 1
Meridian 1 systems to CS 1000M systems

This Meridian 1 system...	Maps to this CS 1000M system
Meridian 1 PBX 11C Chassis	CS 1000M Chassis
Meridian 1 PBX 11C Cabinet	CS 1000M Cabinet
Meridian 1 PBX 51C	CS 1000M Half Group
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 61C CP PII	CS 1000M Single Group
Meridian 1 PBX 81	CS 1000M Multi Group
Meridian 1 PBX 81C	CS 1000M Multi Group
Meridian 1 PBX 81C CP PII	CS 1000M Multi Group

For more information, see one or more of the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258)
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258)
- *Communication Server 1000S: Upgrade Procedures* (553-3031-258)

Intended audience

This document is intended for CS 1000 and Meridian 1 system administrators using a Microsoft Windows®-based PC for management activities. It assumes that you have the following background:

- Working knowledge of the Windows® 2000 server, Windows 2000 Professional, Windows XP Professional operating system
- Familiarity with CS 1000 and Meridian 1 system management activities
- Knowledge of general telecommunications concepts
- Experience with windowing systems or graphical user interfaces (GUI)
- Knowledge of Internet Protocol (IP)

Conventions

Terminology

In this document, the following systems are referred to generically as “system”:

- Meridian 1
- Communication server 1000S (CS 1000S)*
- Communication server 1000M (CS 1000M)*
- Communication server 1000E (CS 1000E)*

The following systems are referred to generically as “Small System”:

- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Communication server 1000M Chassis (CS 1000M Chassis)*
- Communication server 1000M Chassis (CS 1000M Cabinet)*

The following systems are referred to generically as “Large System”:

- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 61C CP PII

- Meridian 1 PBX 81
- Meridian 1 PBX 81C
- Meridian 1 PBX 81C CP PII
- Communication server 1000M Half Group (CS 1000M HG)*
- Communication server 1000M Single Group (CS 1000M SG)*
- Communication server 1000M Multi Group (CS 1000M MG)*

* Systems that are referred to as “CS 1000”

IMPORTANT!

For Communication server 1000 Release 4.0, many terms have been rebranded. However, in this document, the term Optivity NMS (ONMS) has not been rebranded (it appears as it did for Succession 1000 Release 3.0).

The rebranded CS 1000 Release 4.5 term for Optivity NMS (ONMS) is Enterprise Network Management System.

Text

In this document, the following text conventions are used:

angle brackets (< >) Indicates that you must input some command text. You choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is `chg suppress_alarm` <*n*> where *n* is 0 = all, 1 = minor, 2 = major, 3 = critical, you enter `chg suppress_alarm 3` to suppress all alarms except critical alarms.

bold
Courier text Indicates command names, options, and text.

Example: Enter **`prt open_alarm`**.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. **Example:** For additional information, refer to *Using Optivity Telephony Manager.*
plain Courier text	Indicates command syntax and system output, for example, prompts and system messages. **Example:** `Open Alarm destination #0 is 47.82.40.237`
separator (>)	Shows menu paths. **Example:** Select Utilities > Backup in the Navigator window.

Acronyms

The following are some of the acronyms used in this document:

API	application programming interface
ASP	active server page
CCCR	consolidated call cost reports
CLAN	customer local area network (see Nortel server subnet*)
CLI	command line interface
CRS	Consolidated Reporting System
DBA	Data Buffering and Access
DN	directory number
ELAN	embedded local area network
FTP	file transfer protocol
GCAS	General Cost Allocation System
GUI	graphical user interface
IIS	internet information services
I/O	input/output
IP	Internet Protocol
ITG	Internet Telephony Gateway
LAN	local area network
LDAP	lightweight directory access protocol

MAT	Meridian Administration Tools
MIB	management information base
NIC	Network Interface Card
NMS	network management system
OTM	Optivity Telephony Manager
PTY	pseudo-TTY (network port)
RAS	remote access server
RU	reporting unit
SNMP	simple network management protocol
SSL	secure sockets layer
TBS	Telecom Billing System
TLAN	telephony local area network
TN	terminal number
TTY	teletype (serial port)
uid	unique identifier in LDAP synchronization
VPN	Virtual Private Network
VLAN	virtual local area network
WAN	wide area network

*Nortel server subnet, formerly known as CLAN. It is the subnet to which the OTM Network interface is connected.

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Meridian 1 Integrated Telephony Gateway Trunk 1.0/Basic Per-Trunk Signaling: Description, Installation, and Operation* (553-3001-116)

  Describes configuration and maintenance of the Voice Gateway Media card.

- *Meridian 1 Integrated Telephony Gateway Line Card 1.0/IP Telecommuter: Description, Installation, and Operation* (553-3001-119)

  Describes configuration and maintenance of the IP line card for IP Telecommuter.

- *Features and Services* (553-3001-306)

  Describes features associated with systems. For each feature, information is provided on feature implementation, feature operation, and interaction between features.

- *Software Input/Output: Administration* (553-3001-311)

  Describes the prompts and responses for a system's command line interface (CLI). This guide includes information on overlay programs that are classified as administration overlays.

- *Optivity Telephony Manager: System Administration* (553-3001-330)

  Provides information on using the applications and features available with Optivity Telephony Manager on systems.

- *Optivity Telephony Manager: Telemanagement Applications* (553-3001-331)

  Provides information on the following optional telemanagement applications; Telecom Billing System (TBS), TBS Web Reporting, General Cost Allocation System (GCAS), Consolidated Reporting System (CRS), and Consolidated Call Cost Reports (CCCR).

- *IP Trunk: Description, Installation, and Operation* (553-3001-363)

  Describes configuration and maintenance of the Voice Gateway Media card. This card appears as a 24-port trunk card with ISDN Signaling Link (ISL) and D-channel signaling.

- *IP Line: Description, Installation, and Operation* (553-3001-365)

  Describes configuration and maintenance of gateway cards.

- *Telephones and Consoles: Description, Installation, and Operation* (553-3001-367)

  Describes telephones and related features. The telephones provide access to an OTM-generated Corporate Directory.

- *DECT: Description, Planning, Installation, and Operation* (553-3001-370)

  Provides an overview of OTM for Nortel Integrated DECT (DECT) systems.

- *Software Input/Output: System Messages* (553-3001-411)

  Describes the meaning of system messages.

- *Software Input/Output: Maintenance* (553-3001-511)

  Describes the prompts and responses for a system's command line interface (CLI). This guide includes information on overlay programs that are classified as maintenance overlays.

- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)

  Provides information on the Survivable IP Expansion (SIPE) feature for a Meridian 1 Large System.

- *Communication Server 1000S: Installation and Configuration* (553-3031-210)

  Provides information on the Survivable IP Expansion (SIPE) feature for CS 1000S systems.

- *Converging the Data Network with VoIP* (553-3001-160)

  Provides information for Data Networking on Communication server 1000 and Meridian 1 sytems.

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support** on the Nortel home page:

www.nortel.com/

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Preparing for installation

Contents

This chapter contains information on the following topics:

Overview

This chapter contains information on the following topics:

- Installation tasks
- Supported systems
- Supported upgrade paths
- OTM hardware requirements
- OTM software requirements
- License management

Before installing OTM 2.2 Software, please read all of this chapter.

About OTM

OTM combines with the Optivity Network Management System (NMS) to give an integrated data, voice, and video network, as part of the Nortel Unified Networking system. The resulting integration provides converged LAN, WAN, and voice management, and the capacity to monitor OTM server activity through the Optivity NMS.

For installation recommendations to create a secure environment for your OTM data and users, see "Security Management" in the Common Services chapter of *Optivity Telephony Manager: System Administration* (553-3001-330).

To configure modems for use with OTM, refer to "Configuring a modem for OTM applications" on page 153.

When planning OTM installations, consider detailed hardware and software guidelines in Appendix A.

OTM installation tasks

Installing OTM involves performing tasks related to:

- new OTM server software
- new client software
- upgrades
- migrations
- Web Help
- license management

These tasks are covered in detail in the coming chapters.

Supported systems

OTM 2.2 supports the following machine types and managed sytem software releases:

Table 2
OTM-supported machine types and managed system software (Part 1 of 2)

Machine types	X11 software releases	X21 software releases
11C	21, 23, 24, 25	3
11C MINI	24, 25	3
11C Compact	Compact release 1, 2	
51C 030	21, 23	
51C 040	21, 23, 24, 25	
51C 060	23, 24, 25	3
51C 060E	23, 24, 25	3
61C 030	21	
61C 040	23, 24, 25	
61C 060	23, 24, 25	3
61C 060E	23, 24, 25	3
61C PII		3
81, 81C 030	21, 23	
81, 81C 040	21, 23, 24, 25	
81, 81C 060	23, 24, 25	3
81, 81C 060E	23, 24, 25	3
81C PII	25	3
Communication server 1000S		2,3
Communication server 1000		4

Table 2
OTM-supported machine types and managed system software (Part 2 of 2)

Communication server 1000M Multigroup	4
Communication server 1000M	3,4

OTM supports the following systems and components:

- Meridian ITG Trunk 1.0 (OTM IP Telephony M1 IP Trunks application)
- Meridian ITG Trunk 2.0 to 2.2 (OTM IP ISDN IP Trunks application)
- Meridian IP Trunk 3.0/3.01 (OTM ISDN IP Trunk application)
- Meridian ITG Line 1.0 (OTM IP M1 Telecommuter application)
- Meridian ITG Line 2.0 to 2.2 (OTM IP Phones application)
- Meridian IP Line 3.0, 3.1 and 4.0
- DECT (DMC8 card, and DMC4 with updated loadware)
- Meridian 802.11 Wireless IP Gateway (OTM ITG Wireless Application)

Note: OTM concurrence follows the life cycle plans of the Meridian 1 and CS 1000 systems and components with which it inter-works. Some CPU/X11 release/system configurations that have reached their end of life cycle, and thus are not supported by Nortel, are also not supported by OTM.

Supported upgrade paths

OTM 2.2 supports a direct upgrade from OTM 1.20.26, 2.00.50, 2.01.37, and 2.10.56 directly to OTM 2.2.

Direct upgrades are NOT supported for customers migrating from OTM releases prior to 1.20.26. A two-step upgrade is required, first to OTM 2.0 or 2.01 and then to 2.2.

Upgrade from MAT pre-6.67 to OTM 2.2 is purchased new and done as a new install. Upgrade from MAT 6.67 to OTM 2.2 is done as a new install through an upgrade code.

OTM server and clients overview

OTM supports both web and Windows® clients. The Windows GUI interface has more functionality than the web browser interface. The Windows GUI interface may be used directly on the OTM server, or on an OTM Windows® client.

The OTM client accesses and modifies data that is stored on the OTM server. This data is made available by sharing the OTM folder on the OTM server with all OTM clients. Due to the large amounts of data transferred between the OTM server and the OTM clients, high network bandwidth is consumed. Response time and performance will degrade significantly unless the OTM client and OTM server are on the same LAN. In general, a WAN connection is not suitable. Consult "Appendix A: OTM engineering guidelines" in this document for further details on bandwidth and other network requirements for the OTM client communicating with the OTM server. The appendix also provides information on the different network configurations that are possible.

The web clients operate as thin clients connecting directly to a web server running on the OTM server. All operations performed using a web client are executed on the OTM server. The OTM server requires connectivity to the ELAN subnets of the systems being managed.

Atypical client-server architecture

The OTM client is a thick client that runs on a Windows PC. It does not operate in a traditional client-server model. Rather, the OTM client runs similar software to that running on the OTM server. The OTM client communicates directly with the managed systems, and therefore:

- requires connectivity to the ELAN subnets of those systems
- must be operational at the time any operations performed on the client are scheduled to run
- if a site/system defines a serial profile for Station Admin, then there must be physical serial connections between the switch and the server, and between the switch and the client PCs. Communications profiles are defined on a site/system basis and are shared by a server and its clients.

OTM hardware requirements

Refer to "Appendix A: OTM engineering guidelines" for more information on OTM hardware requirements.

Use correct information

The information in this document is subject to change. For the latest system requirements, see the OTM General Release Bulletin.

Ask the network card manufacturer about the type of network card and the availability of the required software driver.

Response-time testing is based upon the recommended configuration, not the minimum configuration. Response-time performance is supported only on the recommended configuration.

For a Windows client some variables are:

- amount of RAM on the OTM client PC
- the Operating System (OS) on the OTM client PC
- number of TNs being managed through the Station Administration application
- other applications that may be running on the OTM client PC, including those that run in the background such as antivirus software
- amount of traffic on the LAN
- the NIC on the OTM client PC
- deployment in the network architecture (topology and placement of the OTM client PC with respect to the OTM server)

The minimum and recommended CPU and RAM configurations are specified. Some OTM applications can run with less than the recommended configurations, but performance may be degraded.

The OTM server requires the following minimum hardware specifications listed in Table 3.

Table 3
OTM server hardware requirements (Part 1 of 2)

Requirement	server configuration	Single (stand alone) configuration	client configuration
Recommended CPU	Intel Pentium III Processor 600 MHz	Intel Pentium III Processor 600 MHz	Intel Pentium III Processor 600 MHz
Minimum CPU	Intel Pentium III Processor 400 MHz	Intel Pentium III Processor 400 MHz	Intel Pentium III Processor 400 MHz
Recommended RAM	512 MB	256 MB, 512 MB	256 MB, 512 MB
Minimum RAM	256 MB	256 MB	256 MB
Hard Drive Space	2 GB (1 GB plus customer data storage)	2 GB (1 GB plus customer data storage)	500 MB
Custom Help	512 MB	512 MB	512 MB
SVGA Color Monitor and interface card	800 X 600 or higher resolution	800 X 600 or higher resolution	800 X 600 or higher resolution
CD-ROM drive	Required	Required	Required
Ethernet Network Interface Card	1 or 2	1	1

Table 3
OTM server hardware requirements (Part 2 of 2)

Requirement	server configuration	Single (stand alone) configuration	client configuration
Hayes- compatible modem is optional for connection to remote sites, required for polling configurations. Please note: WinModems *are incompatible and are not supported.*	56K BPS recommended	56K BPS recommended	56K BPS recommended
PC COM port with 16550 UART [1]	Required	Required	Required
Dongle or USB dongle	Required Supports one USB dongle only USB dongles are not supported through a USB hub	Required Supports one USB dongle only USB dongles are not supported through a USB hub	Not required
Parallel printer port (configured) or USB port (required for dongle)	Required	Required	Required
Two-button Windows-compatible mouse or positioning	Required	Required	Required
Floppy disk	Required	Required	Required

For external modems or direct connection, the PC must have an available serial port (that is, one not being used by a mouse or other serial device). The number of on-board PC

COM ports required depends on the number of external modems or direct connections required.

OTM software requirements

Novell

The OTM server is not supported on a Novell server. TCP/IP communication is supported. IPX/SPX communication is not supported.

General restrictions

- It is the responsibility of the user to ensure that selection of 'Signaling server present' checkbox is completed. OTM cannot automatically determine if a system has a Signaling server.
- For CS 1000M Cabinet and CS 1000M Chassis systems, both appear in OTM as a CS 1000M Small System. Existing fields can be used to differentiate the hardware. The user can:
    - name the system to reflect hardware when adding the system
    - add information into comments field to describe hardware
- The Meridian 1 PBX 11C Chassis (Option 11C Mini) system appears in OTM as a Meridian 1 PBX 11C Cabinet (Option 11C) system after the update system data operation. It is the user's responsibility to select the proper machine type in the system properties page.
- In the **System Data** tab, systems with **Signaling server present** checkbox checked can not be downgraded to non-CS 1000 software releases for ex. X11 Release 25.37. The applicable releases displayed in release combo box is based on the Machine Type and for the CS 1000 machine types only CS 1000 releases are applicable.
- The **Signaling server present** checkbox must be un-checked to downgrade the system to non-CS 1000 software releases.
- If a Meridian 1 system running CS 1000 Release 4.5 in OTM Navigator connects to a system running X11 release software, the non-applicable associated hardware is deleted, and a message for each deleted hardware (Survivable Cabinet and Media Gateways 1000B) is logged in Event Log.

Important restrictions on Windows® XP Professional

Multi-session is not supported. Two users cannot be concurrently logged into the same PC at the same time and have OTM running.

Operating System and application requirements for OTM PC configurations

Table 4, Table 5 on page 44, Table 6 on page 45, and Table 7 on page 47 list the required and supported software that run on OTM PC configuration types.

Table 4
OTM configuration OS requirements

	OTM PC Configuration			
Supported OS Software	**OTM as a server (supporting OTM Windows clients)**	**OTM as a stand alone (supporting no OTM Windows client)**	**OTM as a Windows client**	**OTM web clients**
Windows 2000 server	Yes	Yes	No	Yes
Windows XP Professional	No	Yes	Yes	Yes
Windows 2000 Professional	No	Yes	Yes	Yes

Table 5
OS Service Packs

	OS PC Service Packs
OS software	**Service Pack**
Windows 2000 server	SP4
Windows XP Professional	SP2
Windows 2000 Professional	SP4

Table 6
Application software requirements (Part 1 of 2)

	OTM PC configuration		
Application software	**server**	**Single (stand alone)**	**Windows client**
Internet Explorer 6.0 SP 1 (Windows only) Netscape Communicator 4.79 (UNIX only)	Required	Required	Required
Netscape 6.x or later, Netscape Navigator 4.08	Not supported	Not supported	Not supported
TCP/IP Protocol	Required	Required	Required
RAS (Remote Access Service)	Required	Required	Required
Java 1.4.2 runtime environment	Required	Required	Required
Microsoft Active server Page (ASP)	Required	Required	Required
Communication server 1000 Element Manager	Supported	Supported	Supported
Novell NetWare client 4.8	Supports Windows XP Professional or Windows 2000 Professional	Supports Windows XP Professional or Windows 2000 Professional	Supports Windows XP Professional or Windows 2000 Professional
IIS	IIS 5.0 required for Windows 2000 server	IIS 5.0 required for Windows 2000 IIS 5.1 required for Windows XP Professional	

Table 6
Application software requirements (Part 2 of 2)

	OTM PC configuration		
Application software	**server**	**Single (stand alone)**	**Windows client**
Microsoft Windows Script 5.6	required	required	required

Note 1: Netscape Communicator 4.79 is required on the OTM server and OTM standalone configurations to retrieve the certificate needed for configurations requiring LDAP SSL connection.

Note 2: Nortel does not recommended to run more than one web client from Windows 2000 Professional or Windows XP Professional standalone platforms.

Regional Operating System support

The Windows 2000 server Operating System (OS) is supported for the following languages:

- Japanese
- Simplified Chinese

The Windows 2000 Professional and Windows® XP Professional clients are supported for the following languages:

- Spanish
- French
- German
- Brazilian Portuguese
- Japanese
- Simplified Chinese

Third-party software requirements

Table 7 lists the third party software or firmware included as part of the OTM application.

Table 7
Third-party software requirements

	Software and version	Comments
1	MDAC & Jet Engine 4.0 SP7	MDAC is included in all the supported platforms.
2	Crystal Reports 6.0	
3	JRE 1.4.2	
4	MsXML 4.0 SP2	
5	Sentinel Driver 5.41 used for dongle support.	
6	Pervasive Engines version 8.5 SP2	
7	Netscape Directory SDK version 5.0 for OTM LDAP services and SDK version 5.0 for SSL connection.	
8	Windows Installer 2.0	This is used before OTM is installed on a freshly formatted PC. This is the latest version and it is installed for Windows 2000. It is not installed for Windows XP asince it is included with the OS.
9	ARL (for SNMP) Version 15.3	The Asynchronous Request Library (ARL) provides an API for building SNMP manager applications or for integrating SNMP manager capabilities into an existing application. Basically, it is the SNMP stack for OTM (for all applications).

System software release and package requirements

Table 8 lists OTM software releases and required packages for OTM applications.

Table 8
Meridian 1 X11 system software release and packages

OTM application	Minimum X11 release required	X11 pkgs required
Alarm Management	X11 R22 or later	Pkg 164, 242, 243, and 296
Additional packages for Alarm Notification	N/A	Pkg 55 and 315
Maintenance Windows	X11 R22 or later	Pkg 164, 242, 243, and 296
System Terminal - Overlay Passthru	X11 R22 or later	Pkg 164, 242, and 296
Ethernet connection (for Station Administration, Traffic Analysis, and ESN ART)	X11 R22 or later	Pkg 164, 242, and 296
SMNP Alarms (Open Alarms)	X11 R22 or later	Pkg 315
Data Buffering and Access - Ethernet	X11 R24 or later	Pkg 351
Data Buffering and Access - Serial	N/A	N/A
Database Disaster Recovery	X11 R24 or later	Pkg 164, 242, 296, and 351
Virtual Terminal server	X11 R22 or later for access over IP	Pkg 164, 242, and 296

Table 9 lists CS1000 and Meridian 1 software requirements.

Table 9
CS 1000 and Meridian 1 software requirements

OTM Functionality	X11 Release				CS 1000	Connection Type[1]
	21	23	24	25	2-4	
Maintenance Windows		X	X	X	X	Ethernet/PPP
Alarm Management (windows)	X	X	X	X	X	Ethernet/PPP/Serial
System Terminal:						
Overlay Passthru		X	X	X	X	Ethernet/PPP
VT220	X	X	X	X	X	Serial
ESN Art	X	X	X	X	X	Ethernet/PPP/Serial
Station Administration	X	X	X	X	X	Ethernet/Serial
Traffic Analysis	X	X	X	X	X	Ethernet/Serial[2]
Telecom Billing System (TBS)	X	X	X X	X X	X X	Serial Ethernet (DBA)
Call Tracking	X	X	X	X	X	Serial
Web Alarm Viewing	X	X	X	X	X	Ethernet/PPP
Virtual Terminal server	X	X	X	X	X	Ethernet/PPP/Serial
Maintanence Pages		X	X	X	X	Ethernet/PPP
Web Desktop Services	X	X	X	X	X	Ethernet/Serial
LDAP Sync.						Ethernet
Access server	X	X	X	X	X	Ethernet/PPP/Serial
DECT		X	X	X	X	
1. Ethernet and PPP connections are supported only on Release 22 or later and require the MAT Management Interface software packge 296.						
2. If traffic is being collected through a buffer box , only a serial connection is supported.						

⚠ **CAUTION**

IP Line/IP Trunk file transfers running on CS1000 systems may fail if there is another file transfer protocol (FTP) service running on the OTM server. By default, IIS installs the FTP Publishing Service. This service might be set to start automatically and can cause IP applications to fail.

Installing OTM server software

Contents

This chapter contains information on the following topics:

Overview

This chapter contains information on:

- Installation program features and restrictions
- What to do if there is a problem
- Installing new OTM servers

An installation checklist is provided. See “Appendix B: Installation checklist” on page 327.

IMPORTANT!

OTM 2.2 server software can be installed only on a Windows® 2000 server . See “Windows 2000 server reference” on page 265 for detailed information on installing and configuring operating systems for use with OTM.

You must install OTM web Help separately. See “OTM Web Help” on page 113.

Installation program features

OTM server software installation uses the standard Windows® installation wizard.

Installation messages and log

At the beginning of the OTM server software installation process, the setup program checks for various prerequisites, and displays appropriate messages if one or more required components is not present.

A log records all errors. During installation, the log resides in the following directory path: *C:\NortelLog\log.txt*. After installation, the log resides in the local directory path where you installed the application. For each error or event, the log lists an Event type (for example: Info, Warning, Critical, or Major), and Message (for example: Service Pack 4 is not installed).

Users and groups

During the installation process, OTM adds the Default, EndUser, and HelpDesk user groups to the server. User groups cannot have the same name as a local user on the OTM server. If the installation program detects a local user with the same name as one of the user groups that it is attempting to add, you are given the option of renaming or deleting the local user or canceling the creation of the user group.

CAUTION — Service Interruption

DO NOT install OTM on a Windows® 2000 system that is configured as a primary domain controller (PDC).

Resolving OTM installation problems

If a major problem occurs in the middle of an OTM installation, an unstable system could prevent successful completion.

Procedure 1
Resolving OTM installation problems

1. Delete OTM Navigator and Pervasive shortcuts from the StartUp folder.
2. Reboot.
3. Delete the OTM directory (for example: C:\Nortel\OTM).
4. Run regedit and delete the "HKEY_LOCAL_MACHINE\SOFTWARE\Normat" key.
5. Reboot.
6. Re-install OTM. Execute the setup file. To do this, double-click the *Setup.exe* file on the OTM CD-ROM.

End of Procedure

Installing OTM software

Procedure 2
Installing OTM software

1. Configure the Windows® OS for OTM installation by completing the following steps:

   a. Log on to Windows as an Administrator.

   b. Exit all Windows programs and disable any virus detection software.

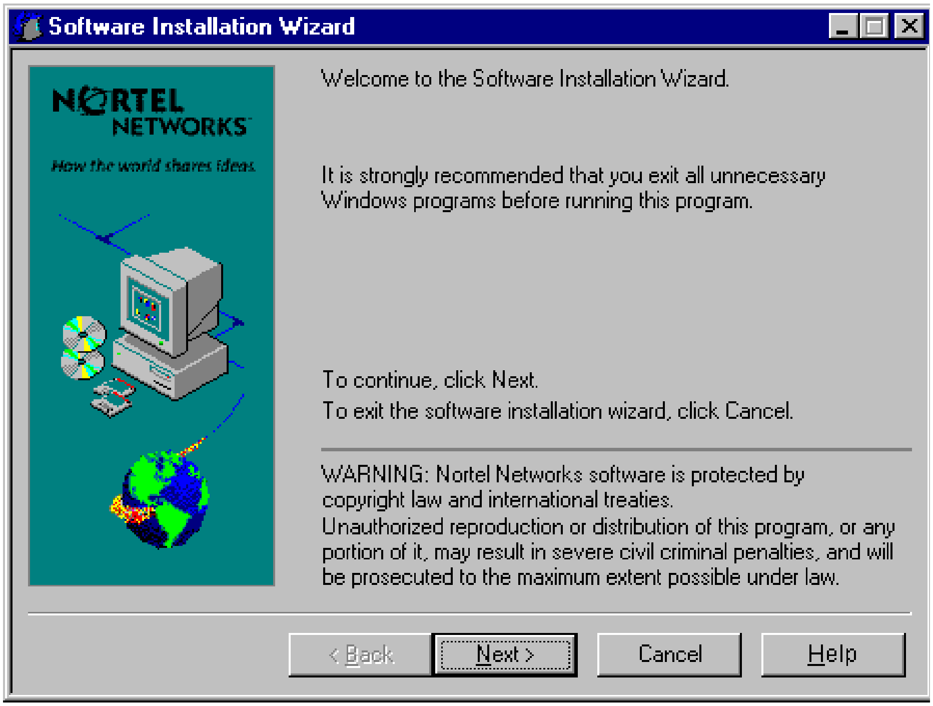
   c. Install the latest Windows critical security updates from Microsoft at http://www.microsoft.com/technet/. The OTM installation wizard does not install the index server, but other applications can install an index server.

   d. Install security patches as advised through Product Bulletins available on the Partner Information Center website.

   Note: Ensure that a drive labeled “C” exists on the server. Although the OTM software can be installed on any drive, there are some dependencies on the C drive. In particular, the directory C:\dbcnv is created during installation and removed at the end of the installation process.

   e. Double-click **Setup.exe** on the OTM CD-ROM, Figure 1 appears.

Figure 1
Software Installation Wizard



Software Installation Wizard

Welcome to the Software Installation Wizard.

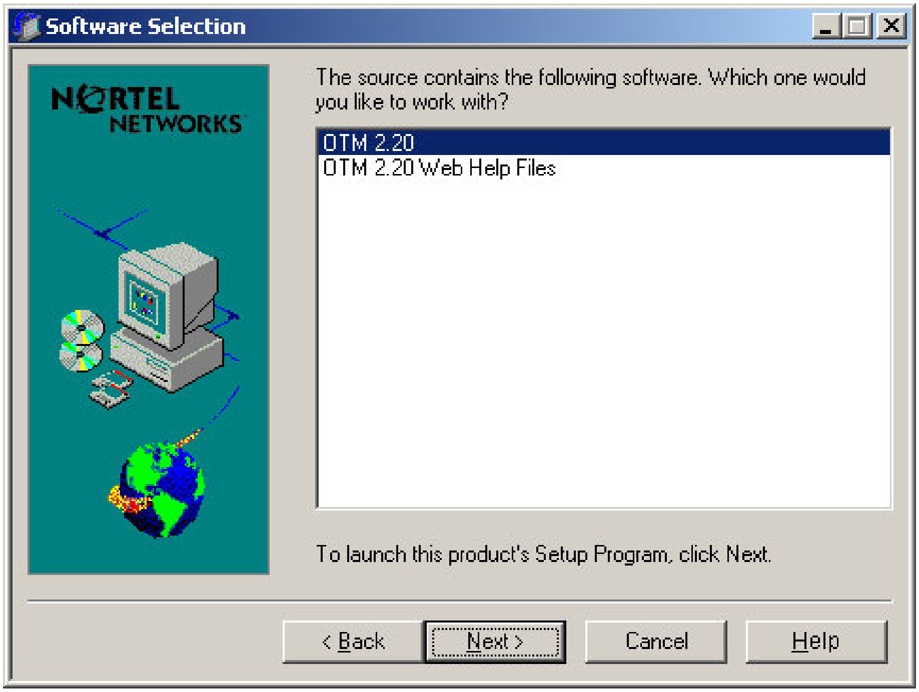
It is strongly recommended that you exit all unnecessary Windows programs before running this program.

To continue, click Next.
To exit the software installation wizard, click Cancel.

WARNING: Nortel Networks software is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil criminal penalties, and will be prosecuted to the maximum extent possible under law.

f. Click **Next** to continue. The Software Selection dialog box appears (Figure 2 on page 55).

Figure 2
Software Selection dialog box



Software Selection

The source contains the following software. Which one would you like to work with?

OTM 2.20
OTM 2.20 Web Help Files

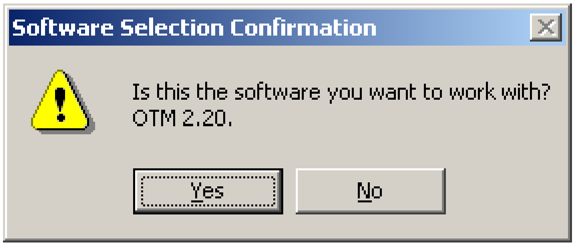
To launch this product's Setup Program, click Next.

2 Click on **OTM 2.20** to select it. Click **Next** to continue.

Note: The other option is OTM web Help files. You can install OTM web Help once the OTM Application installation is complete.

The Software Selection Confirmation dialog box (see Figure 3) opens to request confirmation that OTM 2.2 is the software that you want to work with.

Figure 3
Software Selection Confirmation dialog box



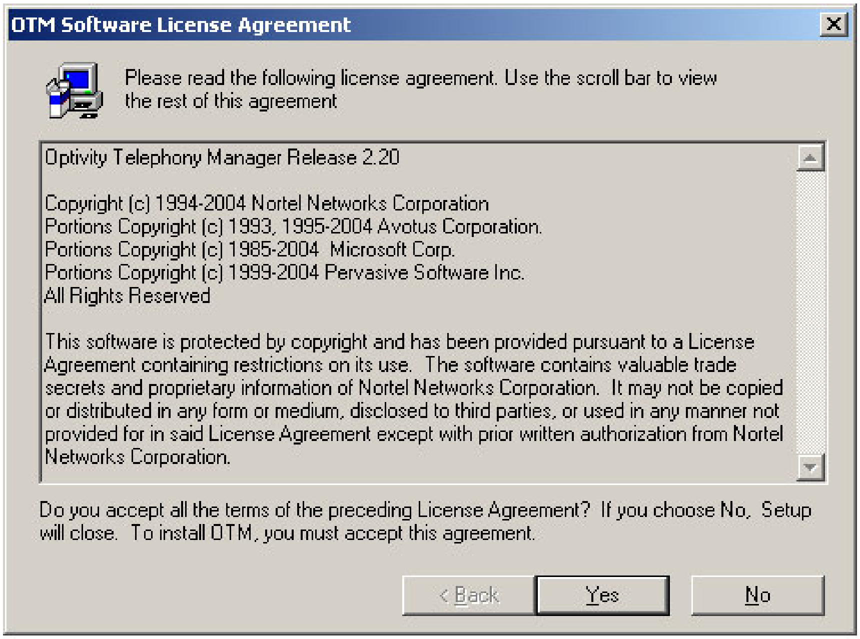
Software Selection Confirmation

Is this the software you want to work with?
OTM 2.20.

3 Click **Yes** to continue.

The software license agreement opens. See Figure 4.

Figure 4
Software License Agreement



OTM Software License Agreement

Please read the following license agreement. Use the scroll bar to view the rest of this agreement

Optivity Telephony Manager Release 2.20

Copyright (c) 1994-2004 Nortel Networks Corporation
Portions Copyright (c) 1993, 1995-2004 Avotus Corporation.
Portions Copyright (c) 1985-2004 Microsoft Corp.
Portions Copyright (c) 1999-2004 Pervasive Software Inc.
All Rights Reserved

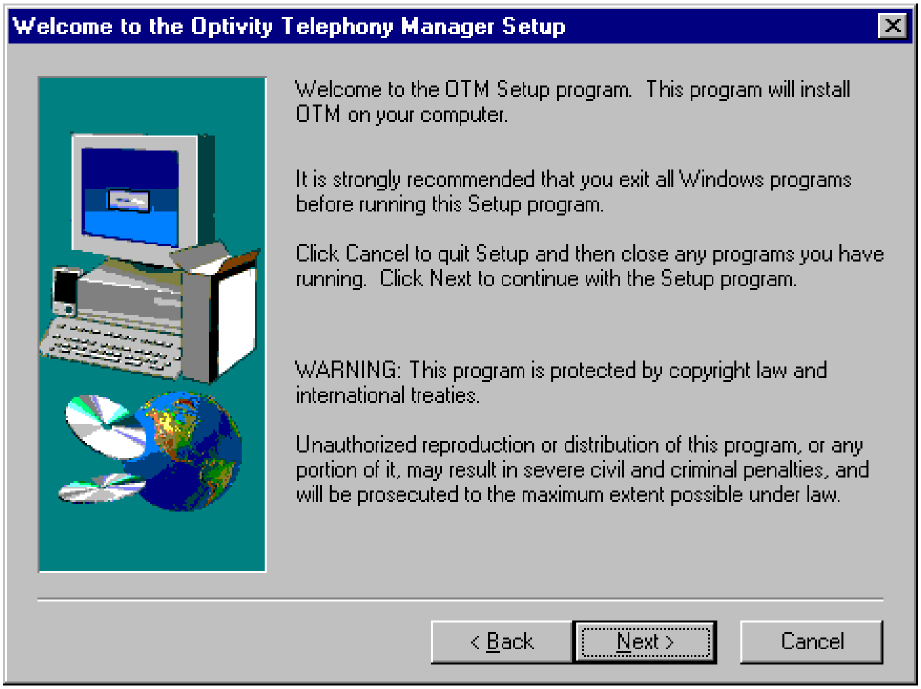
This software is protected by copyright and has been provided pursuant to a License Agreement containing restrictions on its use. The software contains valuable trade secrets and proprietary information of Nortel Networks Corporation. It may not be copied or distributed in any form or medium, disclosed to third parties, or used in any manner not provided for in said License Agreement except with prior written authorization from Nortel Networks Corporation.

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install OTM, you must accept this agreement.

4 Read the license agreement and click **Yes** to accept.

The Welcome screenappears. See Figure 5 on page 57 . It welcomes you to the OTM installation program.

Figure 5
Welcome screen



Welcome to the Optivity Telephony Manager Setup

Welcome to the OTM Setup program. This program will install OTM on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

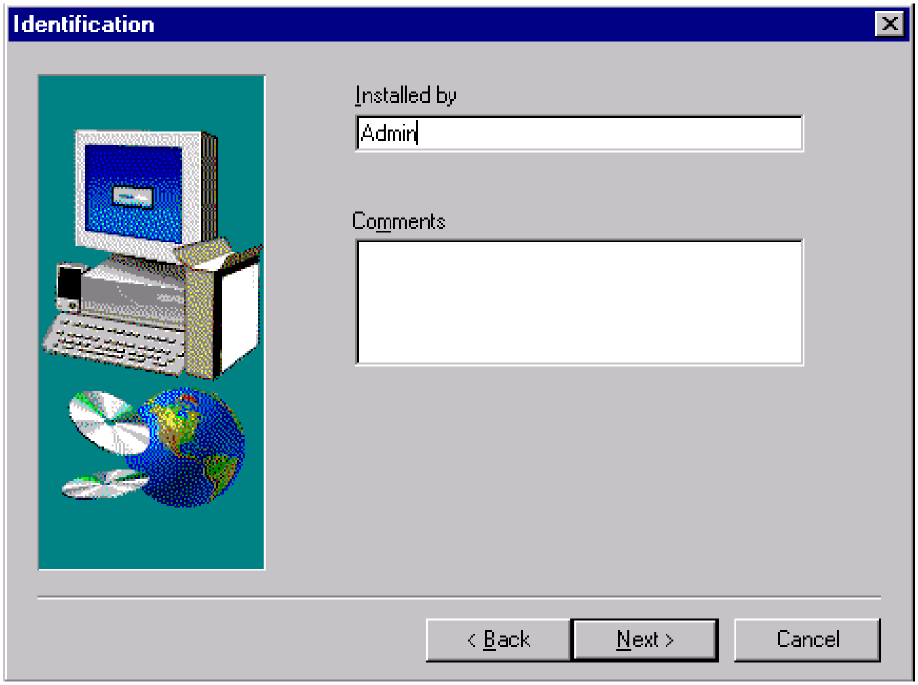
WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

5 Click **Next** to continue.

The Identification screen appears. See Figure 6 on page 58.

Figure 6
Identification screen



Identification

Installed by

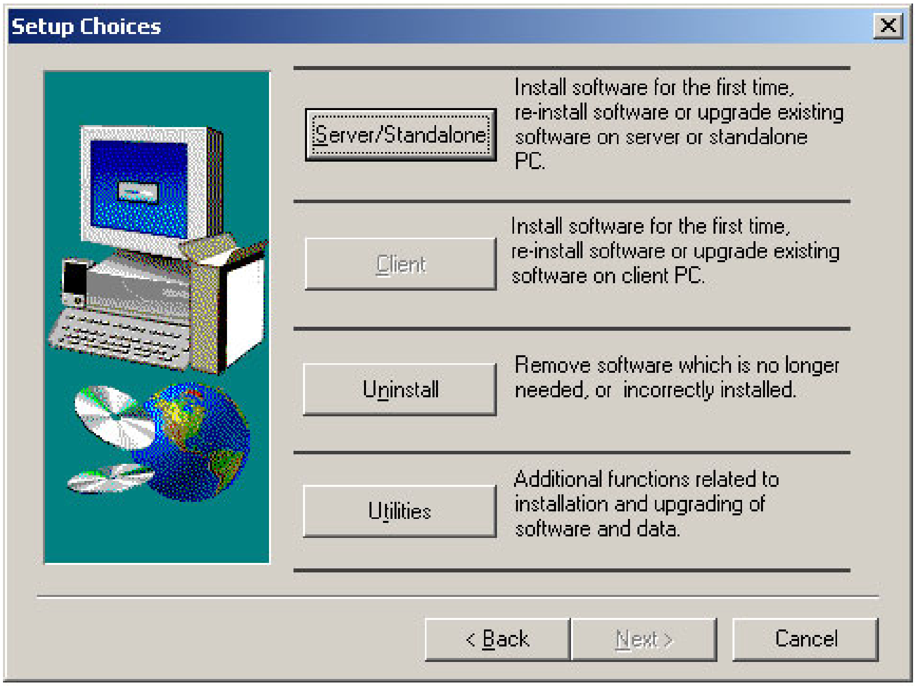
Admin

Comments

6 Specify the name of the person performing the installation and, optionally, a comment about the installation. Click **Next** to continue.

The Setup Choices screen appears. See Figure 7 on page 59.

Figure 7
Setup Choices


Setup Choices

Server/Standalone — Install software for the first time, re-install software or upgrade existing software on server or standalone PC.

Client — Install software for the first time, re-install software or upgrade existing software on client PC.

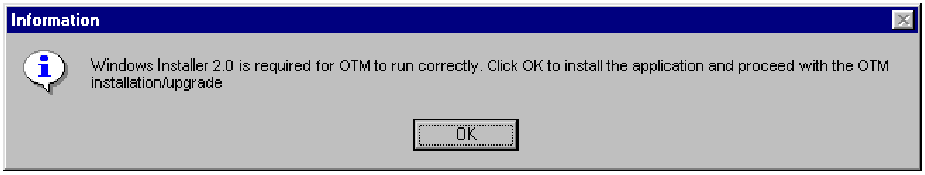
Uninstall — Remove software which is no longer needed, or incorrectly installed.

Utilities — Additional functions related to installation and upgrading of software and data.

7 Make setup choices. For installation on an OTM server, select **server/Standalone**.

OTM requires Windows Installer 2.0. If the installation wizard detects that Windows Installer 2.0 is not installed, the information box shown in Figure 8 on page 59 appears. Click **OK**. OTM installation continues after Windows Installer 2.0 installation has been completed, and the system has been rebooted.

Figure 8
Windows Installer 2.0 information box


Information

Windows Installer 2.0 is required for OTM to run correctly. Click OK to install the application and proceed with the OTM installation/upgrade

IMPORTANT!

Selecting server/Standalone does not resolve problems with damaged software. To resolve a damaged software problem, back up your data files and perform an Uninstall. Next, perform an installation, and then restore your data.

You must have the OTM server software installed prior to installing the client software. The client has applications and executables, but uses the common data from the OTM server.

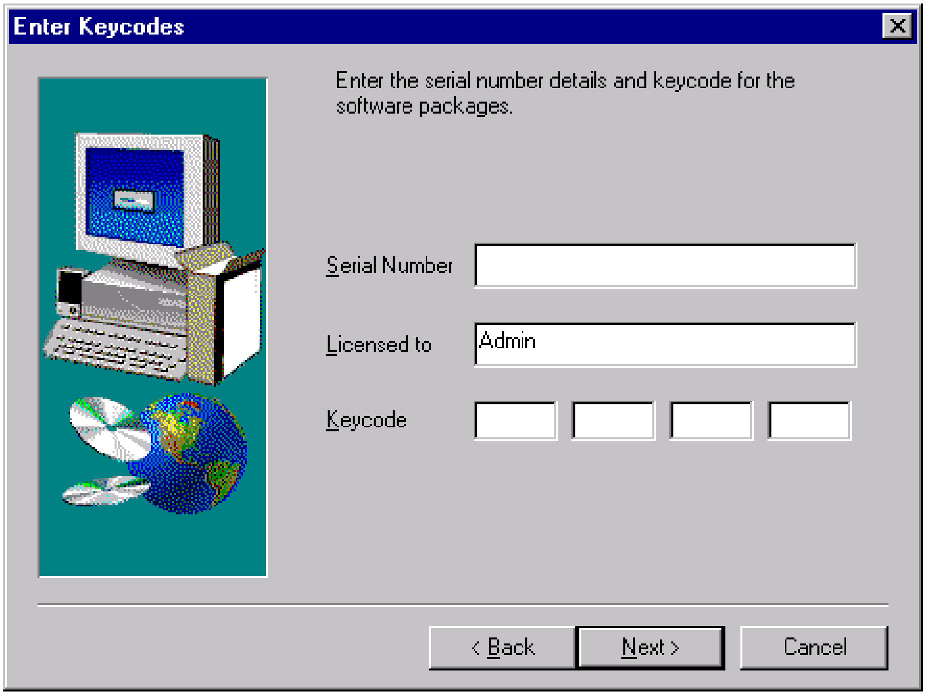
8 Enter the serial number and keycode that you received with your OTM software package in the Enter Keycodes dialog box (Figure 9 on page 61).

Keycodes from a previous OTM keycodes do not work. You must use the latest OTM keycode.

The serial number and keycode determine which applications are installed during the software installation process. The serial number and keycode also determine the maximum number of terminal numbers (TNs), or sets (telephones), and OTM clients that can be configured in your OTM system. In determining your maximum number of TNs, only telephone TNs and virtual TNs are counted. Trunk TNs are not included. To purchase licensing for additional TNs or clients, contact your OTM vendor.

Click **Next** to continue. The Destination for Application Files dialog box appears. See Figure 10 on page 62.

Figure 9
Enter keycode



Enter Keycodes

Enter the serial number details and keycode for the software packages.

Serial Number:

Licensed to: Admin

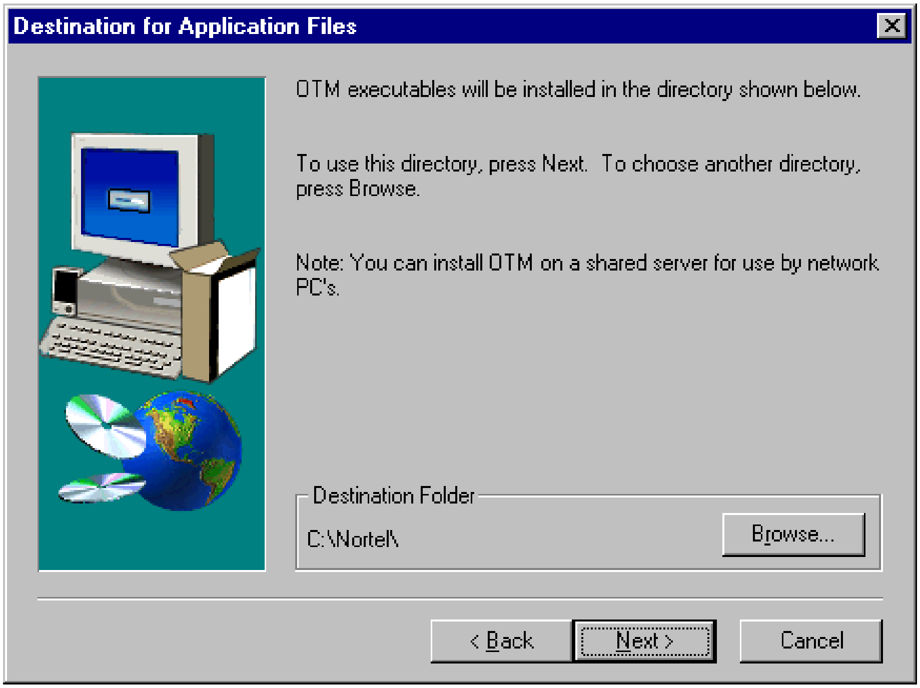
Keycode:

9 Specify a destination (root directory) for application files. Choose one of the following:

a. Use the default directory. Click **Next.** The Destination for Common Data files dialog box appears. See Figure 11 on page 63.

b. Click **Browse,** see Figure 10, to specify a different location. Click **Next**. A window appears “c:\Nortel\ does not exist. Do you want to create it?”. Click **Yes**. The Destination for Common Data files dialog box appears. See Figure 11 on page 63.

Figure 10
Destination for Application Files



Destination for Application Files

OTM executables will be installed in the directory shown below.

To use this directory, press Next. To choose another directory, press Browse.

Note: You can install OTM on a shared server for use by network PC's.

Destination Folder

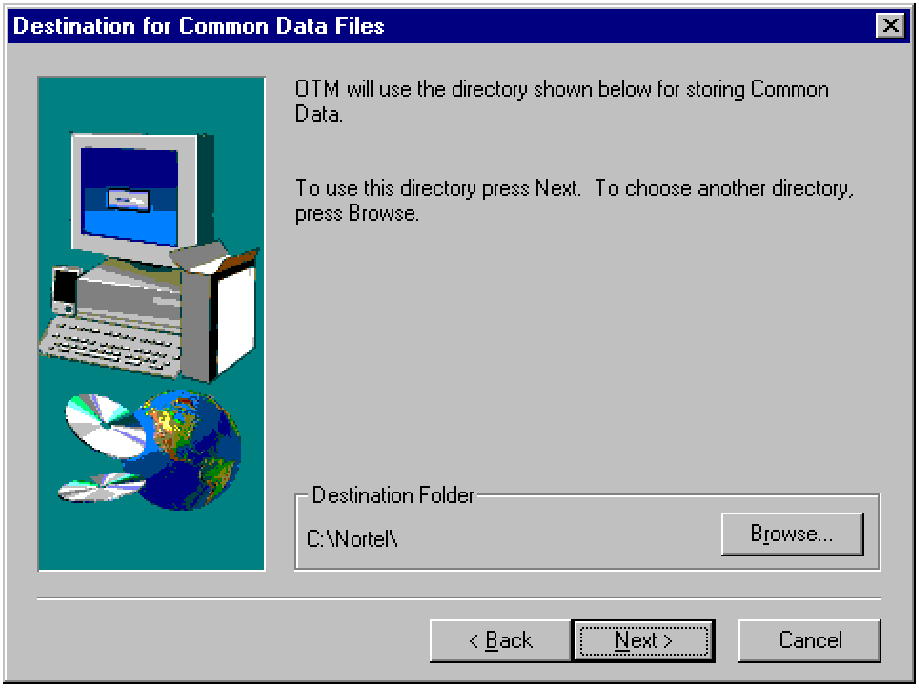
C:\Nortel\

CAUTION — Service Interruption

You must not install OTM in the root directory (for example, C:\). During the installation process, you must specify a folder (for example, C:\Nortel). If you install in the root directory, OTM uninstall attempts to delete everything on the drive.

10 Specify a destination for common data files. Specify the root directory for installing OTM Common Data files. See Figure 11 on page 63. Use the default directory or browse to specify a different location. Click **Next** to continue.

Figure 11
Destination for Common Data Files dialog box



Destination for Common Data Files

OTM will use the directory shown below for storing Common Data.

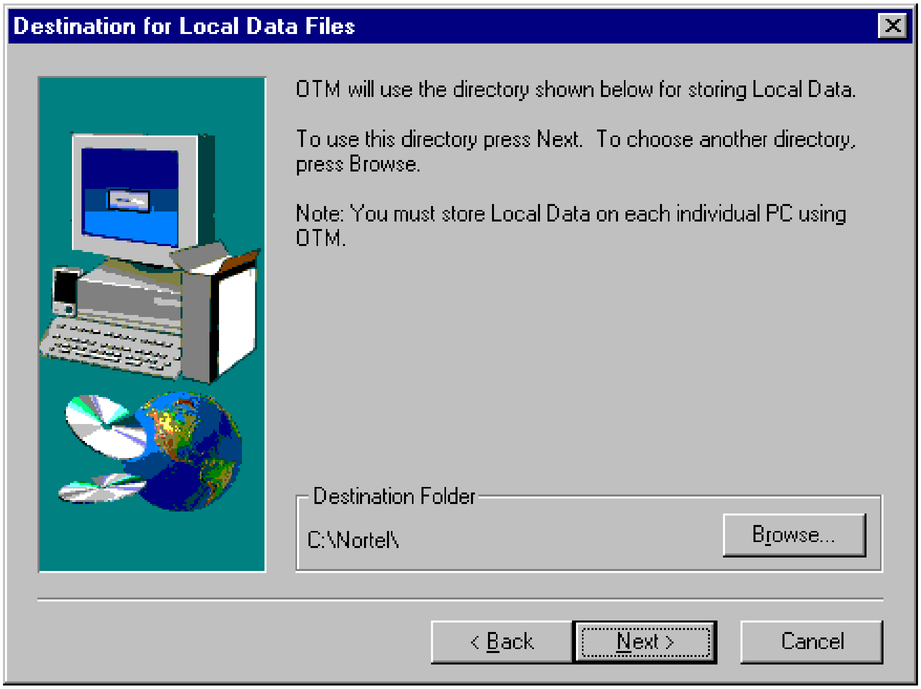
To use this directory press Next. To choose another directory, press Browse.

Destination Folder

C:\Nortel\

11 Specify a destination for local data files. Specify the root directory for installing OTM Local Data files. See Figure 12 on page 64. Use the default directory or browse to specify a different location. Click **Next** to continue.

Figure 12
Destination for Local Data Files dialog box



Destination for Local Data Files

OTM will use the directory shown below for storing Local Data.

To use this directory press Next. To choose another directory, press Browse.

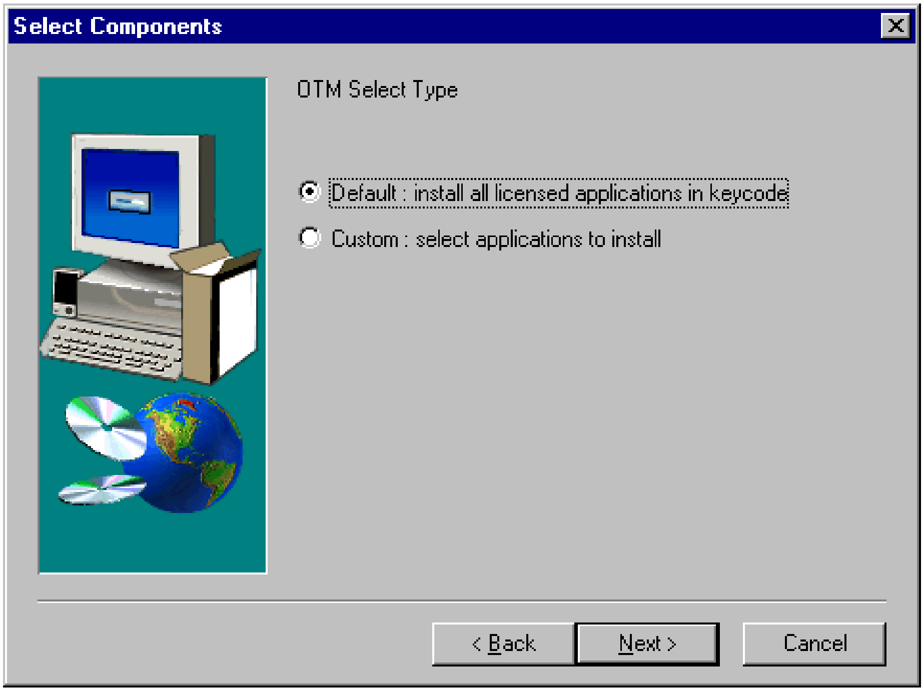
Note: You must store Local Data on each individual PC using OTM.

Destination Folder

C:\Nortel\

12 Specify installation options. See Figure 13 on page 65.

Figure 13
Select Components



Select Components

OTM Select Type

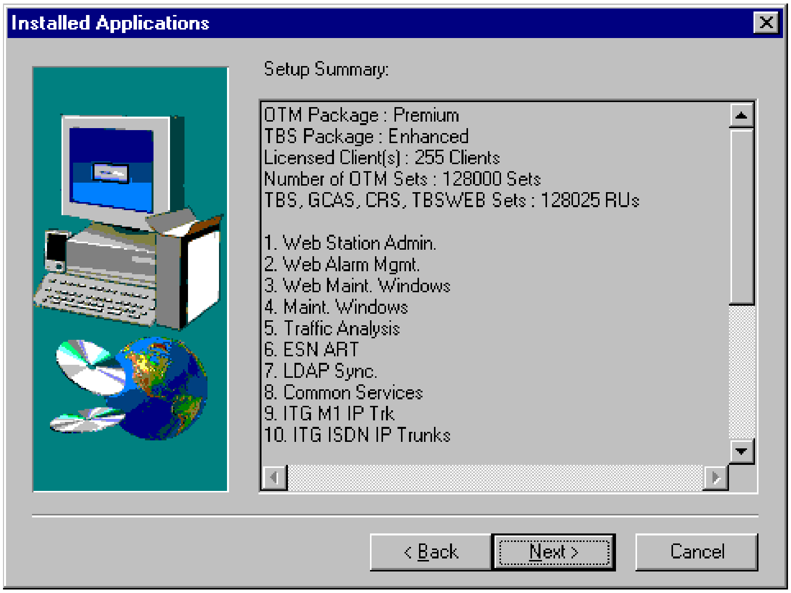
● Default : install all licensed applications in keycode

○ Custom : select applications to install

a. If you select Default, a summary of the default applications for the level of OTM that you have purchased appears. See Figure 14 on page 66. Click **Next** to continue.

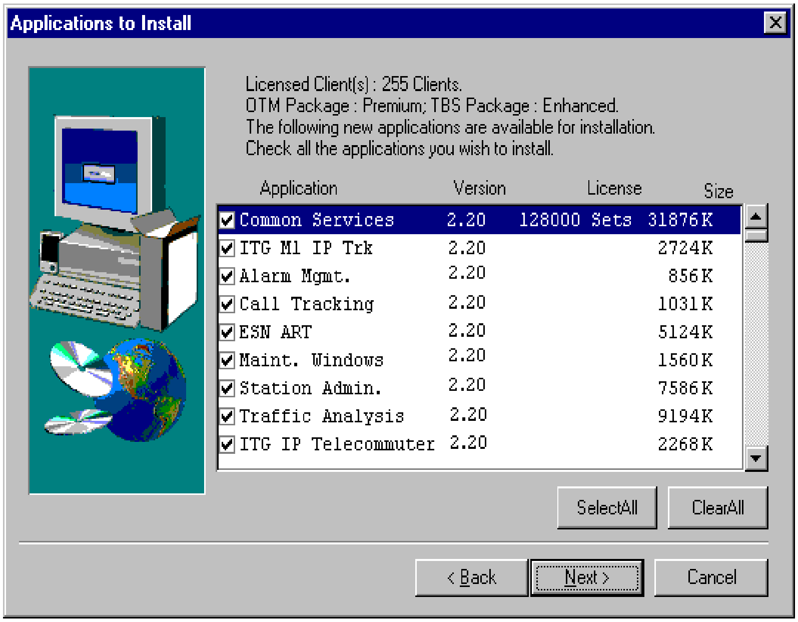
b. If you select Custom, you are given a list of applications to install. See Figure 15 on page 66. Check the appropriate applications and click **Next** to continue.

Figure 14
Summary of default applications



```
OTM Package : Premium
TBS Package : Enhanced
Licensed Client(s) : 255 Clients
Number of OTM Sets : 128000 Sets
TBS, GCAS, CRS, TBSWEB Sets : 128025 RUs

1. Web Station Admin.
2. Web Alarm Mgmt.
3. Web Maint. Windows
4. Maint. Windows
5. Traffic Analysis
6. ESN ART
7. LDAP Sync.
8. Common Services
9. ITG M1 IP Trk
10. ITG ISDN IP Trunks
```

Figure 15
Custom Applications to Install

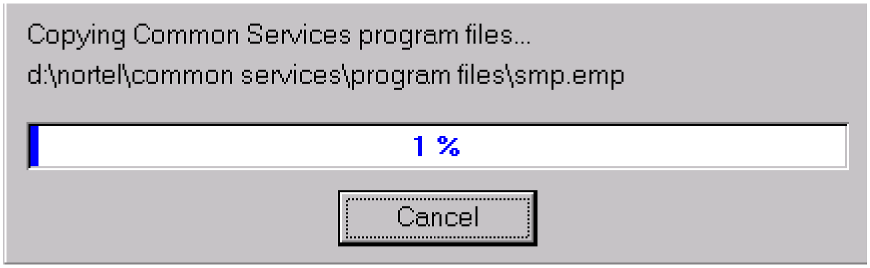


Licensed Client(s) : 255 Clients.
OTM Package : Premium; TBS Package : Enhanced.
The following new applications are available for installation.
Check all the applications you wish to install.

Application	Version	License	Size
☑ Common Services	2.20	128000 Sets	31876K
☑ ITG M1 IP Trk	2.20		2724K
☑ Alarm Mgmt.	2.20		856K
☑ Call Tracking	2.20		1031K
☑ ESN ART	2.20		5124K
☑ Maint. Windows	2.20		1560K
☑ Station Admin.	2.20		7586K
☑ Traffic Analysis	2.20		9194K
☑ ITG IP Telecommuter	2.20		2268K

The Copy files dialog box appears the percentage status of OTM installation, which application files are being copied, and their locations. See Figure 16.

Figure 16
Copy files

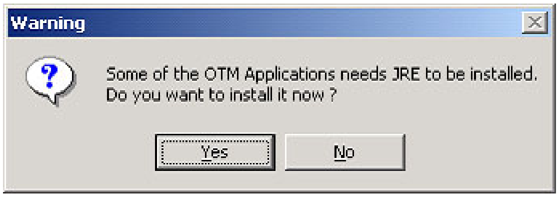


Copying Common Services program files...
d:\nortel\common services\program files\smp.emp

13 A Read Me dialog box prompts you to read the readme.txt file.
Click **Yes** to view the Read Me file or No to skip the Read Me file.

14 If you have installed applications that require Java* Runtime Environment (JRE), you are prompted to install JRE at this point. See Figure 17. Click **Yes** if you want to install JRE now. It is required for the Alarm Script Wizard and the DECT application.

Figure 17
JRE Installation



Warning

Some of the OTM Applications needs JRE to be installed.
Do you want to install it now ?

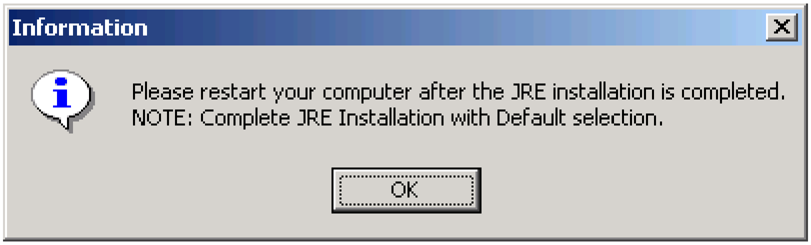
You may decide to install JRE at a later time. The JRE install program is located in the OTM directory (for example, C:\Nortel) at:

- For Windows: *C:\Nortel\OMServices\Jre\Windows\j2re-1_4_2-win.exe*
- To find which version of JRE you have, look under your "control panel > Java plug-in > About box".
- For other operating systems: Support for Java Plug-in Software on other operating systems is provided by the operating system vendor. For more information on Java Plug-in documentation and Frequently Asked Questions, refer to
  http://java.sun.com/.

JRE is required for the Alarm Script Wizard and the DECT application.

15 The JRE Information window opens (Figure 18). Click **OK**.

Figure 18
JRE Information

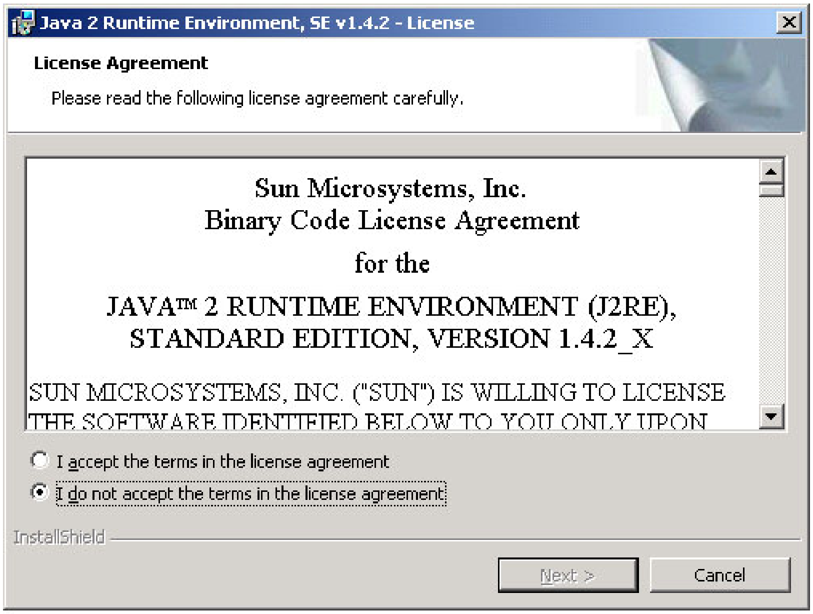


Information

Please restart your computer after the JRE installation is completed.
NOTE: Complete JRE Installation with Default selection.

16 The JRE Licensening Agreement window opens. See Figure 19. Select **I accept the terms in the license agreement**. Click **Next**.

Figure 19
JRE License Agreement



Java 2 Runtime Environment, SE v1.4.2 - License

License Agreement

Please read the following license agreement carefully.

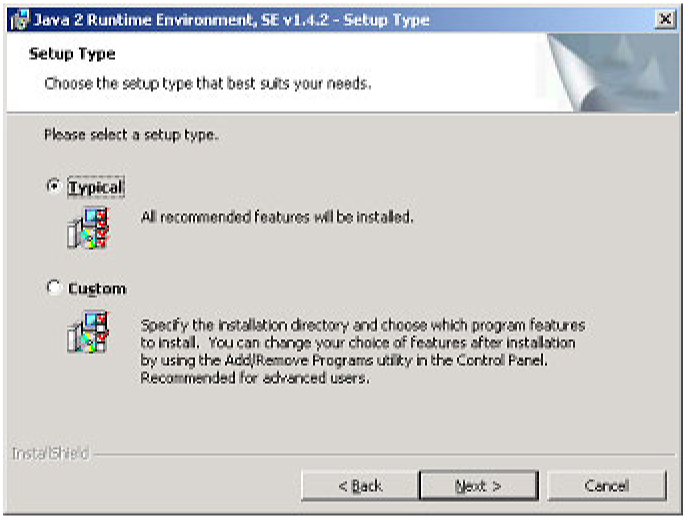
Sun Microsystems, Inc.
Binary Code License Agreement
for the
JAVA™ 2 RUNTIME ENVIRONMENT (J2RE), STANDARD EDITION, VERSION 1.4.2_X

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON

○ I accept the terms in the license agreement
● I do not accept the terms in the license agreement

17 The JRE Setup Type window opens. See Figure 20. Select **Typical** from the JRE Setup Type screen to perform the default JRE installation. Click **Next**. Click **Finish** when install is complete.

Figure 20
JRE Setup Type



Java 2 Runtime Environment, SE v1.4.2 - Setup Type

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● Typical

All recommended features will be installed.

○ Custom

Specify the installation directory and choose which program features to install. You can change your choice of features after installation by using the Add/Remove Programs utility in the Control Panel. Recommended for advanced users.

18 Restart the computer. A dialog box asks you to restart the computer or end the installation without restarting the computer. Select **Yes, I want to restart my computer now**, and click **OK**.

19 Check the installation log to make sure you installed OTM software correctly, and that prerequisites have been met. During installation, the log resides in the following directory path: *C:\NortelLog\log.txt*. After installation, the log resides in the Local Data directory where you installed the application.

End of Procedure

Installing OTM client software

Contents

This chapter contains information on the following topics:

Overview

This chapter contains information on installing OTM client software.

OTM client software installation is similar to the OTM server installation. The steps are summarized in this chapter. See the previous chapter to view the installation screens that are common to both procedures.

OTM server and client's overview

OTM supports both web and Windows clients. The Windows GUI interface has more functionality than the web browser interface. The Windows GUI interface may be used directly on the OTM server, or on an OTM Windows client.

The web clients operate as thin clients connecting directly to a web server running on the OTM server. All operations performed using a web client are executed on the OTM server. The OTM server requires connectivity to the ELAN subnets of the systems being managed.

The OTM client is a thick client that runs on a Windows PC. It does not operate in a traditional client-server model. Rather, the OTM client runs similar software to that running on the OTM server. The OTM client communicates directly with the managed systems, and therefore requires connectivity to the ELAN subnets of those systems. The OTM client must be operational at the time any operations performed on the client are scheduled to run.

The OTM client accesses and modifies data that is stored on the OTM server. This data is made available by sharing the OTM folder on the OTM server with all OTM clients. Due to the large amounts of data transferred between the OTM server and the OTM clients, high network bandwidth is consumed. Response time and performance will degrade significantly unless the OTM client and OTM server are on the same LAN. In general a WAN connection is not suitable.

Consult the Engineering Guidelines in "Appendix A: OTM engineering guidelines" in this document for further details on bandwidth and other network requirements for the OTM client communicating with the OTM server. The appendix also provides information on the different network configurations that are possible.

Installing the software

1 Before installation:

   a. On client PC, exit all Windows programs and disable any virus detection software.

   b. Remove the OTM.exe shortcut file in the Start up folder, if present.

   c. Ensure Distributed COM is enabled. For DCOM to work, the OTM client must be able to reach the OTM server by its actual IP address. If Network Address Translation (NAT) is used on the server, the OTM client is not able to reach the server:

      i. From Control Panel>Administrative Tools>Component Services, right-click **My Computer** under the Computers folder of the Console tree.

      ii. Click on the Default Properties tab, ensure the “Enable Distributed COM on this computer” check box is selected.

   d. On the OTM server, share the Nortel directory with the specific users or user groups who use the OTM client.

CAUTION — Service Interruption

Assign share permissions for the Nortel directory according to your corporate security standards.

   e. On the client PC, map the Nortel directory located on the OTM server.

2 Start the installation. To do this, double-click the **Setup.exe** file on the OTM CD-ROM.

3 Navigate through the OTM installation wizard. The following screens appear (for examples, see “Installing OTM software” on page 53).

   a. Welcome to the Software Installation Wizard

   b. Software selection

   c. Software selection confirmation

d. OTM Software Licence Agreement

e. Welcome to the Optivity Telephony Manager Setup

f. Identification

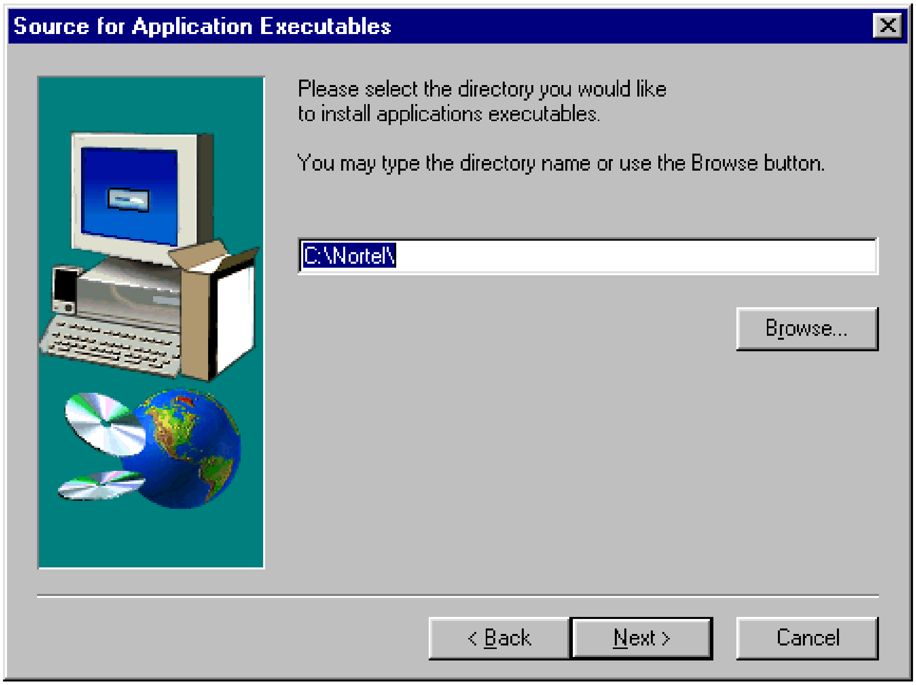
Note: If required, the setup program installs DCOM at this point if it is not present on the PC. Once installed, you must reboot the PC. After you reboot and log in, the OTM software installation continues.

4 In the Setup Choices dialog box, select **client**.

5 Select the directory for the installation of the application executable as shown in Figure 21. You may browse and select a local directory on the client PC, or you can browse and select the mapped OTM server directory. Click **Next** to continue. A Question window appears.

6 Click **Yes** on the dialog window “c:\Nortel\ does not exist. Do you want to create it”.

Figure 21
Source for Application Executables dialog box



Source for Application Executables

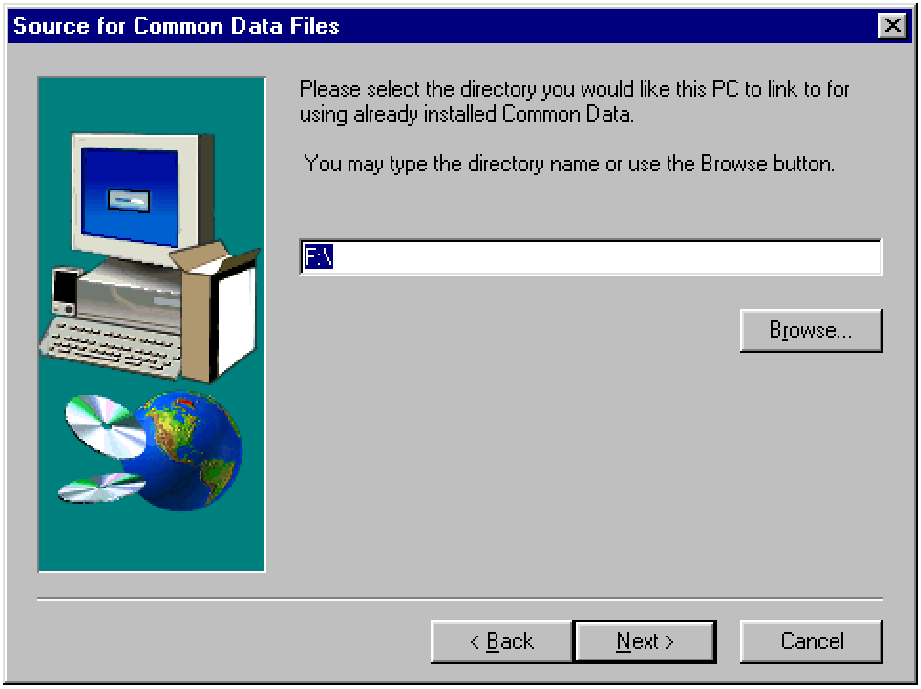
Please select the directory you would like
to install applications executables.

You may type the directory name or use the Browse button.

C:\Nortel\

7 Select the shared directory on the OTM server. See Figure 22 on page 74. Click **Next** to continue.

Figure 22
Source for Common Data Files dialog box



Source for Common Data Files

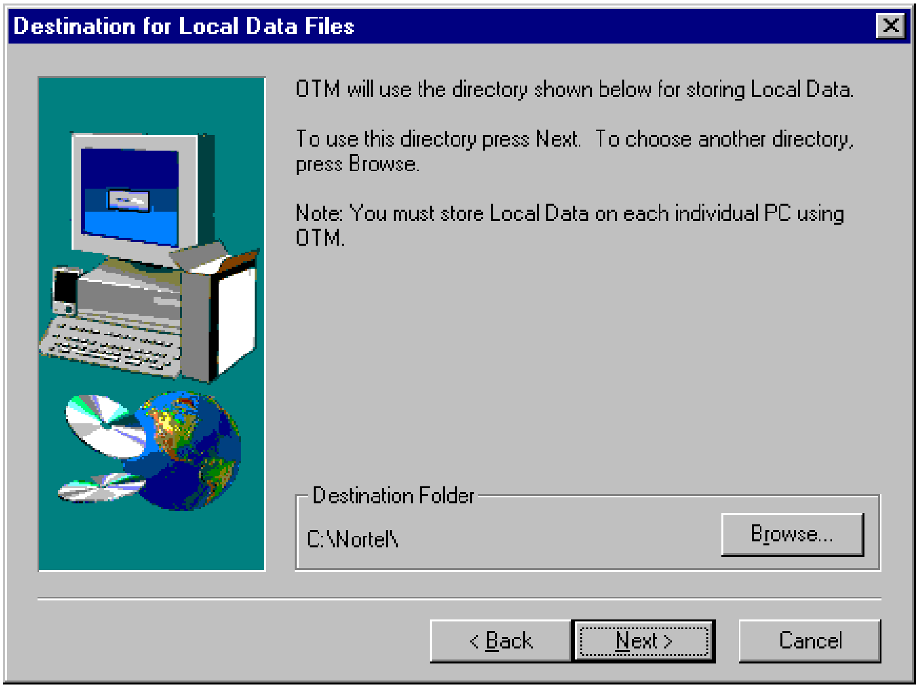
Please select the directory you would like this PC to link to for using already installed Common Data.

You may type the directory name or use the Browse button.

F:\

8 Select the destination on the client PC for the local data files. See Figure 23 on page 75. You must select a directory on the client PC. Click **Next** to continue.

Figure 23
Destination for Local Data Files dialog box



Destination for Local Data Files

OTM will use the directory shown below for storing Local Data.

To use this directory press Next. To choose another directory, press Browse.

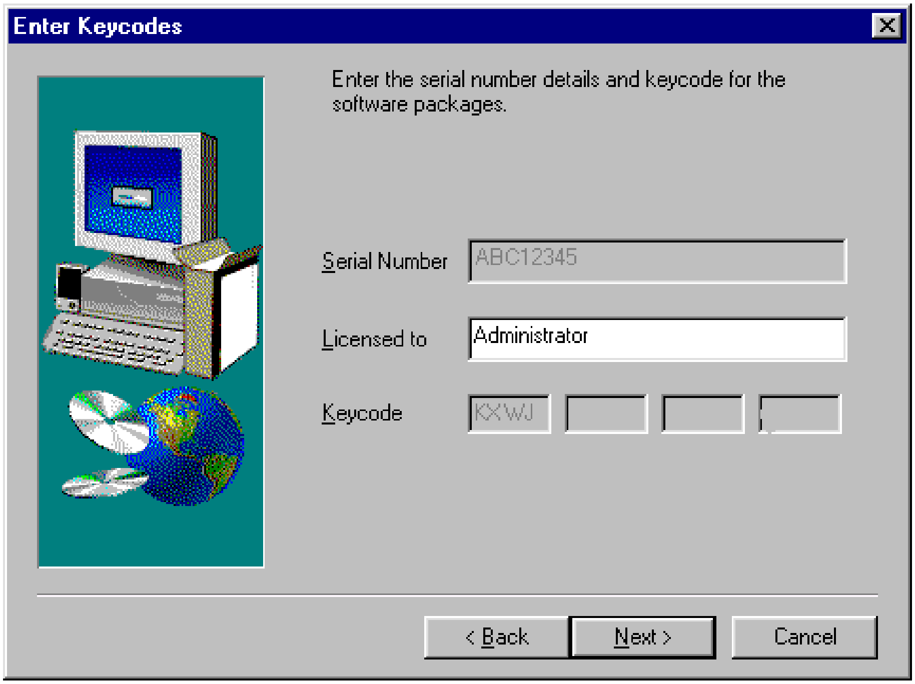
Note: You must store Local Data on each individual PC using OTM.

Destination Folder

C:\Nortel\

9 The Enter Keycodes dialog box appears. See Figure 24 on page 76. The fields contain the data stored on the OTM server. Click **Next** to continue.

Figure 24
Enter Keycodes dialog box



Enter Keycodes

Enter the serial number details and keycode for the software packages.

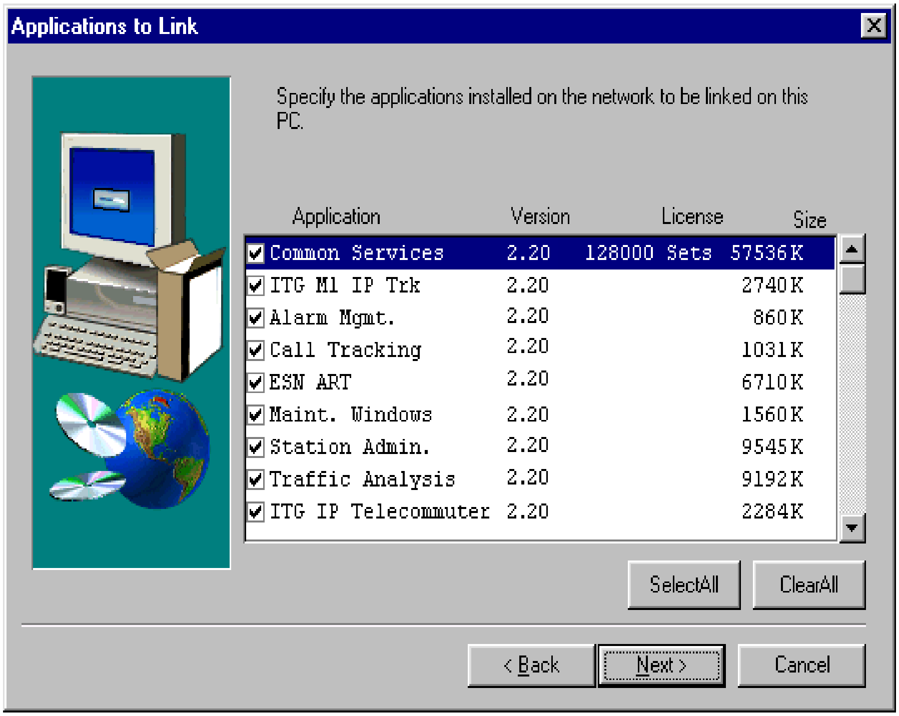
Serial Number: ABC12345

Licensed to: Administrator

Keycode: KXWJ

10 The Applications to Link dialog box appears. See Figure 25 on page 77. Select the applications to be linked to use the applications installed on the OTM server. Click **Next** to continue.

Figure 25
Applications to Link dialog box



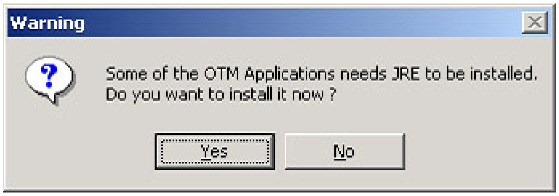
Specify the applications installed on the network to be linked on this PC.

Application	Version	License	Size
☑ Common Services	2.20	128000 Sets	57536K
☑ ITG M1 IP Trk	2.20		2740K
☑ Alarm Mgmt.	2.20		860K
☑ Call Tracking	2.20		1031K
☑ ESN ART	2.20		6710K
☑ Maint. Windows	2.20		1560K
☑ Station Admin.	2.20		9545K
☑ Traffic Analysis	2.20		9192K
☑ ITG IP Telecommuter	2.20		2284K

11 After the installation is complete, you are given the option to view the Read Me file. Click **Yes** to view the Read Me file or **No** to skip the Read Me file.

12 If you have installed applications that require Java* Runtime Environment (JRE), you are prompted to install JRE at this point. See Figure 26. Click **Yes** if you want to install JRE now. It is required for the Alarm Script Wizard and the DECT application.

Figure 26
JRE Installation



Some of the OTM Applications needs JRE to be installed.
Do you want to install it now ?

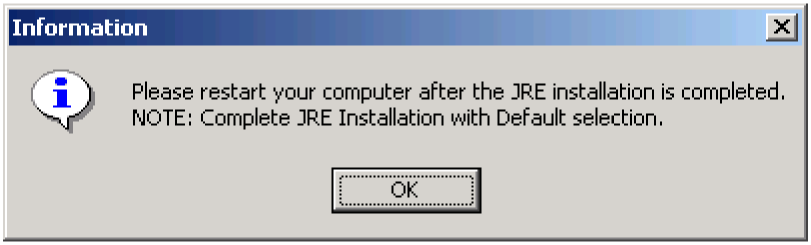
You may decide to install JRE at a later time. The JRE install program is located in the OTM directory (for example, C:\Nortel) at:

- For Windows: *C:\Nortel\OMServices\Jre\Windows\j2re-1_4_2-win.exe*
- To find which version of JRE you have, look under your "control panel > Java plug-in > About box".
- For other operating systems: Support for Java Plug-in Software on other operating systems is provided by the operating system vendor. For more information on Java Plug-in documentation and Frequently Asked Questions, refer to http://java.sun.com/.

JRE is required for the Alarm Script Wizard and the DECT application.

The JRE Information window opens (Figure 27). Click **OK**.

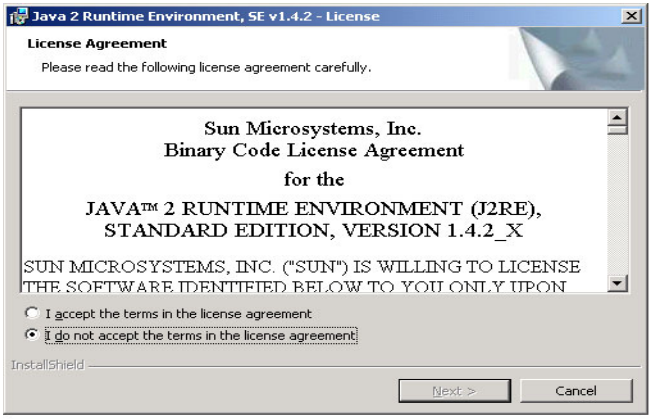
Figure 27
JRE Information



Please restart your computer after the JRE installation is completed.
NOTE: Complete JRE Installation with Default selection.

13 The JRE Licensening Agreement window opens (Figure 28). Select **I accept the terms in the license agreement**. Click **Next**.

Figure 28
JRE License Agreement



Java 2 Runtime Environment, SE v1.4.2 - License

License Agreement

Please read the following license agreement carefully.

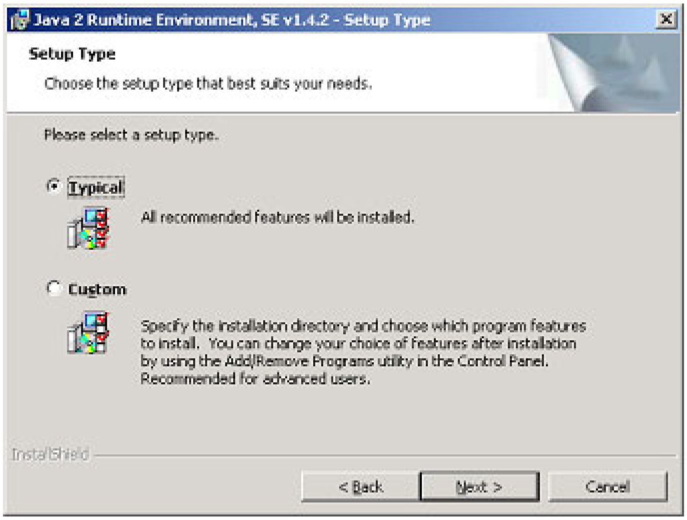
Sun Microsystems, Inc.
Binary Code License Agreement
for the
JAVA™ 2 RUNTIME ENVIRONMENT (J2RE),
STANDARD EDITION, VERSION 1.4.2_X

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON

○ I accept the terms in the license agreement
● I do not accept the terms in the license agreement

14 The JRE Setup Type window opens. See Figure 29. Select **Typical** from the JRE Setup Type screen to perform the default JRE installation. Click **Next**. Click **Finish** when install is complete.

Figure 29
JRE Setup Type



Java 2 Runtime Environment, SE v1.4.2 - Setup Type

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● Typical
All recommended features will be installed.

○ Custom
Specify the installation directory and choose which program features to install. You can change your choice of features after installation by using the Add/Remove Programs utility in the Control Panel. Recommended for advanced users.

15 Restart the computer. A dialog box asks you to restart the computer or end the installation without restarting the computer. Select **Yes, I want to restart my computer now**, and click **OK**.

16 Check the installation log to make sure you installed OTM software correctly, and that prerequisites have been met. During installation, the log resides in the following directory path: *C:\NortelLog\log.txt*. After installation, the log resides in the Local Data directory where you installed the application. .

Note

To avoid mis-alignment of pages when printing multiple pages of designation strips in station administration, please perform the following steps.

1. After installation/upgrade of OTM, uninstall the "Generic/Text only" printer.

2. Reboot the PC.

3. Re-install the "Generic/Text only" printer.

4. Reboot the PC.

End of Procedure

pcAnywhere uninstallation

When pcAnywhere version 11.0 is installed on a system and later it is uninstalled, DCOM service is disabled by the uninstall process. This process fails OTM login.

To enable OTM login, complete the following procedure:

Once the pcAnywhere version 11.0 is uninstalled, re-enable the DCOM service.

Procedure 3
Re-enable the DCOM service

1 Go to **Control Panel->Administrative Tools->Component Services**

2 Click **Computers** folder

3 Right-click on **My Computer**.

4 Select **Properties**.

5 Select **Default Properties** tab.

6 Place a check next to "Enable Distributed COM on this computer".

7 Click **OK** and close the Component Services window.

8 Reboot the machine for the changes to take effect.

End of Procedure

Performing upgrades

Contents

This chapter contains information on the following topics:

Overview

This chapter contains information on upgrading the following:

- OTM server
- OTM PCs
- OTM software

The upgrade installation is very similar to the initial installation.

You need a new keycode to upgrade to another OTM package or to increase the maximum number of OTM clients and sets (telephones).

IMPORTANT!

The OTM server and client software must be the same version. If the server software is upgraded, the client software must also be upgraded.

IMPORTANT!

Following an upgrade, only locally authenticated users can launch OTM. Remotely authenticated users cannot. Refer to Procedure 30 on page 173 for more information on allowing remote users to gain access.

IMPORTANT!

Users who belong to the Administration group in OTM 1.2 will be migrated to the Administrators group after upgrading to OTM release 2.0 or higher. These users will therefore gain OS administrative rights after the upgrade.

If you do not want OTM administrators to share OS administrative rights, create a new user group and move these users to the new group.

For more information on administrative rights for users, see “Administrators” on page 164.

Upgrading the OTM server to the same release of OTM

Upgrade the OTM server for the following reasons:

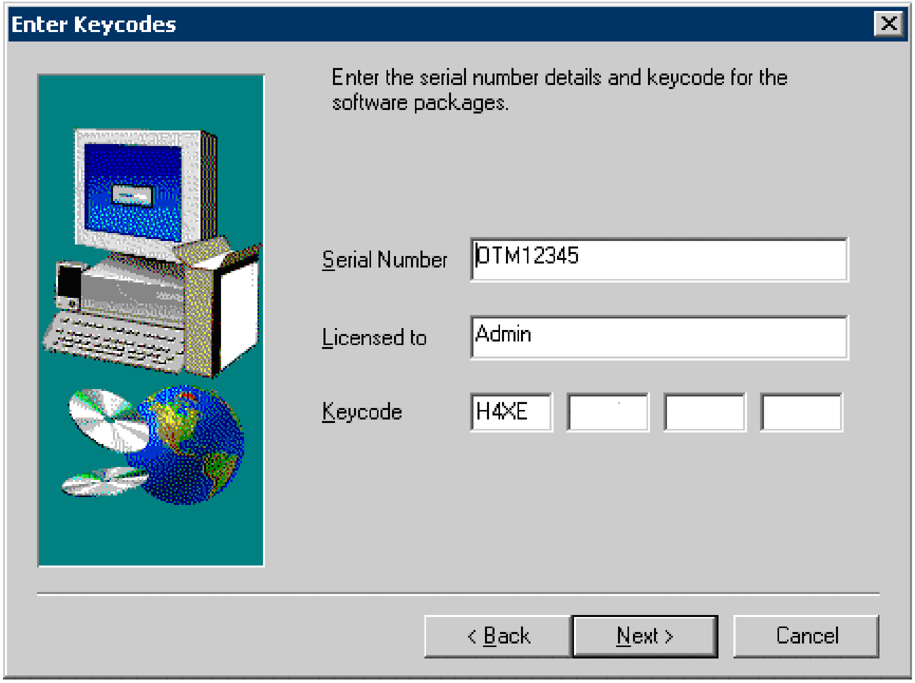
- to install OTM applications not previously installed
- to upgrade to another OTM package (for example, from General to Premium)
- to amend TN licenses and Reporting Units

Procedure 4
Installing OTM applications not previously installed

If an upgrade is done on a server in a client server setup, close all OTM client applications and OTM server applications, then reboot the server.

1. Double-click **Setup.exe** on the OTM CD-ROM.
2. Navigate through the OTM installation wizard. The following screens appear (see “Installing OTM software” on page 53).
    a. Welcome to the Software Installation Wizard
    b. Software selection
    c. Software confirmation
    d. OTM Software Licences Agreement
    e. Welcome to the Optivity Telephony Manager Setup
    f. Identification
    g. Setup Choices
3. Enter the serial number and keycode that you received with your OTM software package in the Enter Keycodes dialog box. See Figure 30 on page 84. Click **Next** to continue.

Figure 30
Enter Keycodes dialog box



Enter Keycodes

Enter the serial number details and keycode for the software packages.

Serial Number: OTM12345

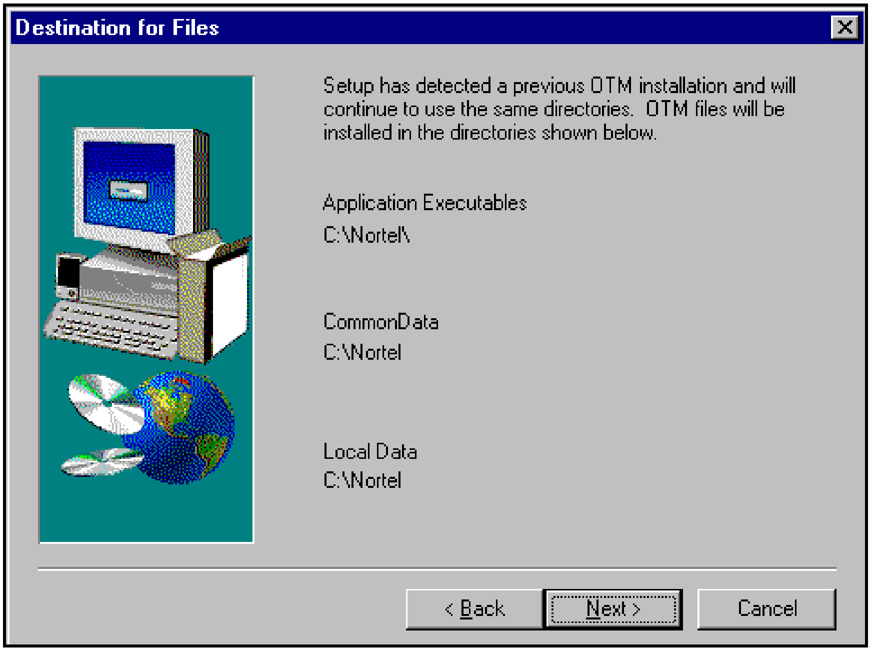
Licensed to: Admin

Keycode: H4XE

Note: Previous OTM keycodes do not work. You must use the new OTM keycode.

The **Destination for Files** dialog box appears. The directory path of the previously selected Application files, Common Data files, and Local Data files are shown. See Figure 31 on page 85.

Figure 31
Destination for Files dialog box



Destination for Files

Setup has detected a previous OTM installation and will continue to use the same directories. OTM files will be installed in the directories shown below.

Application Executables
C:\Nortel\

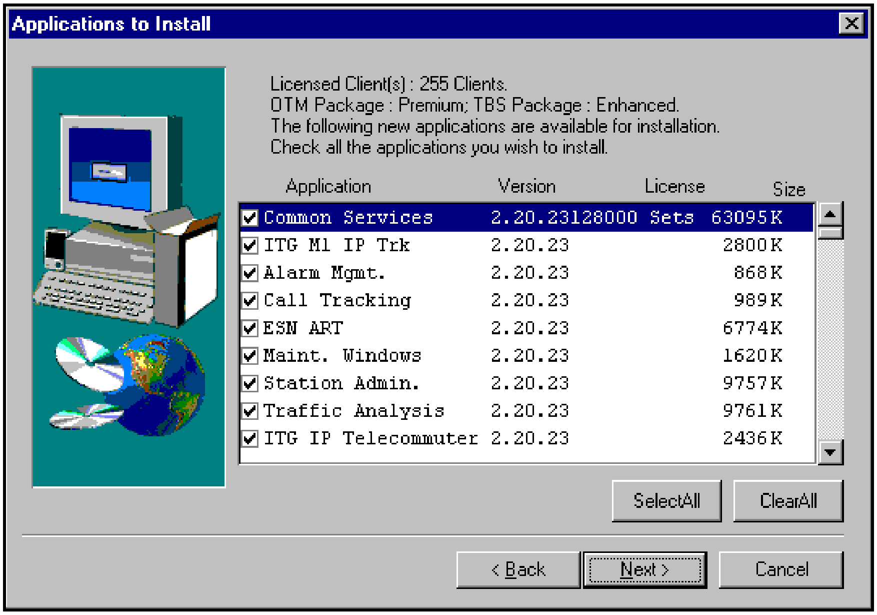
CommonData
C:\Nortel

Local Data
C:\Nortel

4 Click **Next** to continue.

The list of left-out applications which were not selected during installation is displayed. See Figure 32 on page 86.

Figure 32
Applications to Install dialog box



Applications to Install

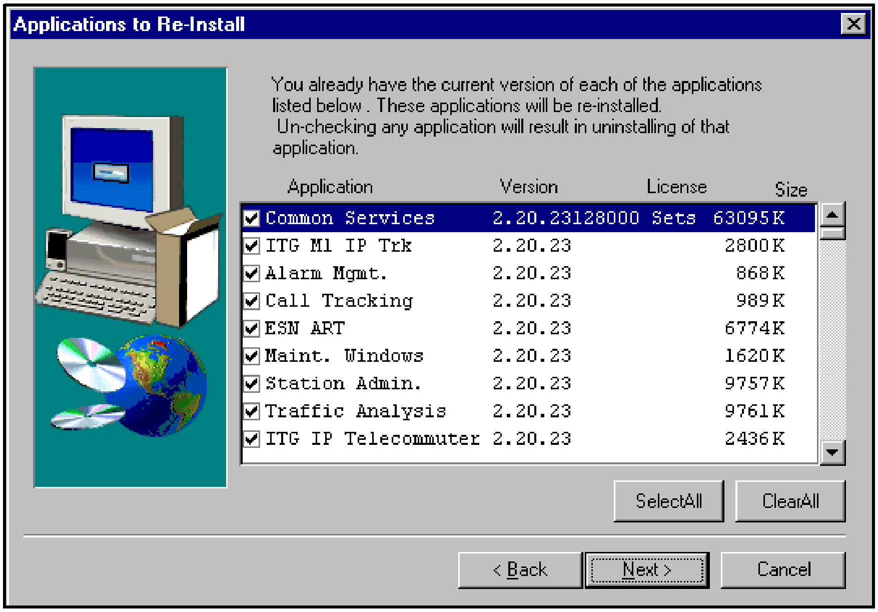
Licensed Client(s) : 255 Clients.
OTM Package : Premium; TBS Package : Enhanced.
The following new applications are available for installation.
Check all the applications you wish to install.

Application	Version	License	Size
☑ Common Services	2.20.23	128000 Sets	63095K
☑ ITG M1 IP Trk	2.20.23		2800K
☑ Alarm Mgmt.	2.20.23		868K
☑ Call Tracking	2.20.23		989K
☑ ESN ART	2.20.23		6774K
☑ Maint. Windows	2.20.23		1620K
☑ Station Admin.	2.20.23		9757K
☑ Traffic Analysis	2.20.23		9761K
☑ ITG IP Telecommuter	2.20.23		2436K

5 Select the applications you need to add. Click **Next** to continue.

The list of installed applications is displayed. See Figure 33 on page 87.

Figure 33
Applications to Re-Install

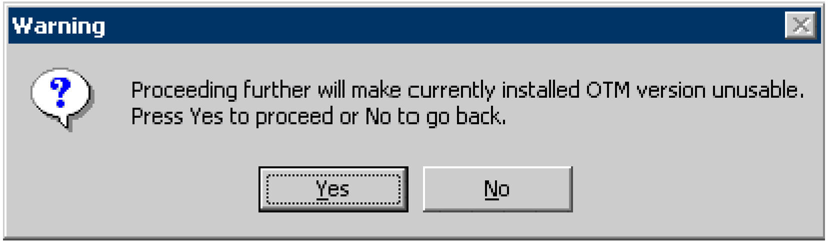


You already have the current version of each of the applications listed below . These applications will be re-installed.
Un-checking any application will result in uninstalling of that application.

	Application	Version	License	Size
☑	Common Services	2.20.23	128000 Sets	63095K
☑	ITG M1 IP Trk	2.20.23		2800K
☑	Alarm Mgmt.	2.20.23		868K
☑	Call Tracking	2.20.23		989K
☑	ESN ART	2.20.23		6774K
☑	Maint. Windows	2.20.23		1620K
☑	Station Admin.	2.20.23		9757K
☑	Traffic Analysis	2.20.23		9761K
☑	ITG IP Telecommuter	2.20.23		2436K

6 Make any modifications to the selected applications. All the check boxes are selected by default. Clearing any check box uninstalls that particular application. Click **Next** to continue.

Figure 34
Warning message



Proceeding further will make currently installed OTM version unusable.
Press Yes to proceed or No to go back.

7 The Warning message appears. See Figure 34. Choose one of the following:

a. Click **Yes** to continue. Proceed to step 9.

b. Click **No** to go back.

8 A window dialog box appears stating that some DLL files are in use and the PC needs to be re-booted. Choose one of the following:

   a. Click **Yes** to reboot the PC. Repeat the following steps:

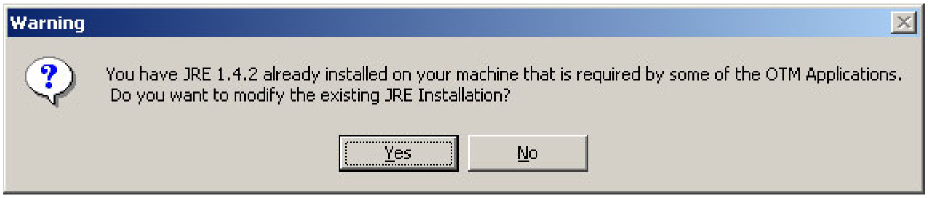
      - Software License Agreement
      - Welcome to the Optivity Telephony Manager setup
      - Identification
      - Setup Choices
      - Enter Keycodes
      - Destination for Files
      - Application to Install
      - Applications to Re-Install
      - Warning.

   b. Click **No** to stop the installation.

9 A Read Me dialog box prompts you to read the readme.txt file.
Click **Yes** to view the Read Me file or **No** to skip the Read Me file. Close the Readme.txt to continue.

10 If you have installed applications that require Java* Runtime Environment (JRE), you are prompted to install JRE at this point. See Figure 35. Click **Yes** if you want to install JRE now. JRE is required for the Alarm Script Wizard and the DECT application.

Figure 35
JRE Installation



Warning

You have JRE 1.4.2 already installed on your machine that is required by some of the OTM Applications.
Do you want to modify the existing JRE Installation?

You may decide to install JRE at a later time. The JRE install program is located in the OTM directory (for example, C:\Nortel) at:

- For Windows: *C:\Nortel\OMServices\Jre\Windows\j2re-1_4_2-win.exe*
- For other operating systems: Support for Java Plug-in Software on other operating systems is provided by the operating system vendor. For more information on Java Plug-in documentation and Frequently Asked Questions, refer to http://java.sun.com/.

JRE is required for the Alarm Script Wizard and the DECT application.

After clicking **Yes**, a Limits Updated window appears asking you to restart your computer after the JRE installation is completed.

11 Click **OK** to continue.

The Java 2 Runtime Environment installShield Wizard for Java 2 appears.

12 Click **Next** to continue. The Program Maintenance window appears.

13 Select **Modify** to modify previously installed JAVA applications .

14 Click **Next.** The Custom Setup window appears.

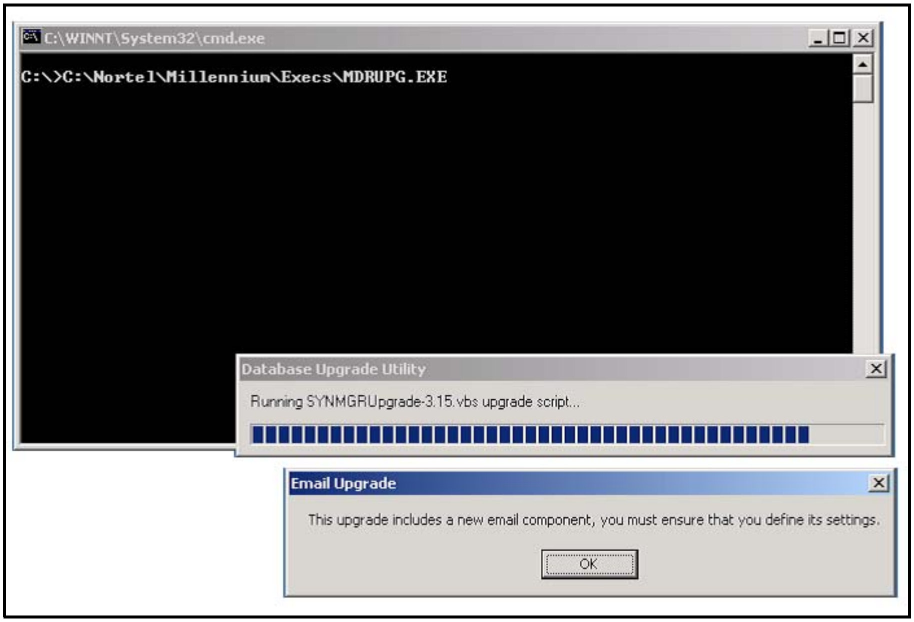
15 Click on **Next** to continue.The Progress window appears where Java is being installed.

16 Click **Finish** to complete installation.

17 Restart the computer. A dialog box asks you to restart the computer or end the installation without restarting the computer. Select **Yes**, **I want to restart my computer now**, and then click **OK** to continue.

18 After reboot , a message, see Figure 36, appears if a Database Upgrade Utility or Email Upgrade has run, reminding you to define its settings.

Figure 36
Upgrade message



```
C:\>C:\Nortel\Millennium\Execs\MDRUPG.EXE
```

Database Upgrade Utility

Running SYNMGRUpgrade-3.15.vbs upgrade script...

Email Upgrade

This upgrade includes a new email component, you must ensure that you define its settings.

Note

To avoid mis-alignment of pages when printing multiple pages of designation strips in station administration, please perform the following steps.

1. After installation/upgrade of OTM, uninstall the "Generic/Text only" printer.

2. Reboot the PC.

3. Re-install the "Generic/Text only" printer.

4. Reboot the PC.

End of Procedure

Upgrading to another OTM package

Procedure 5
Upgrading to another OTM package

If an upgrade is done on a server in client server setup, close all OTM client applications and OTM server applications, then reboot the server.

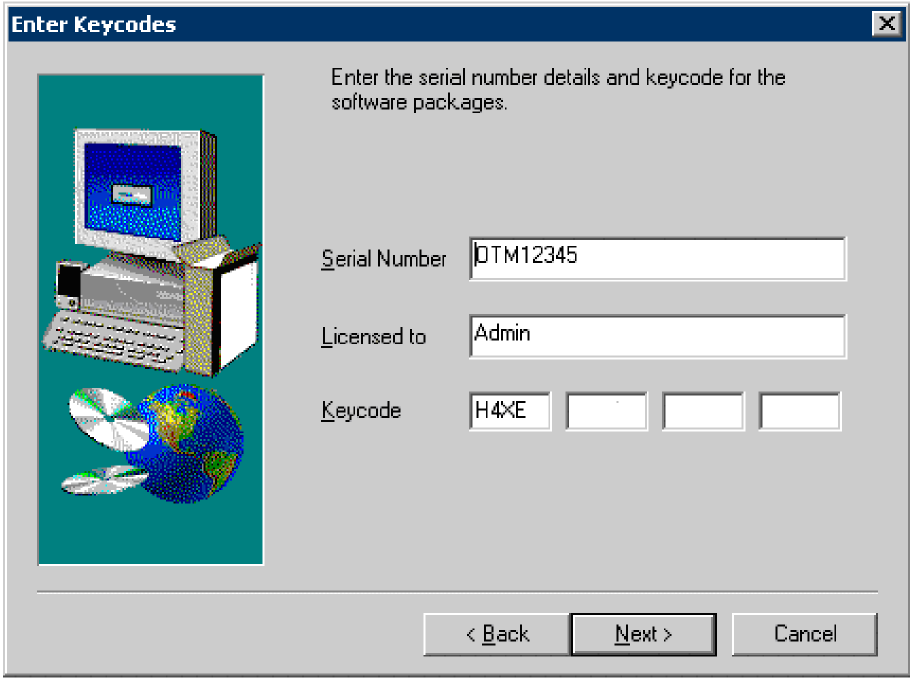
1 Double-click **Setup.exe** on the OTM CD-ROM.

2 Navigate through the OTM installation wizard. The following screens appear (see "Installing OTM software" on page 53).

- **a.** Welcome to the Software Installation Wizard
- **b.** Software selection
- **c.** Software selection confirmation
- **d.** OTM Software Licences Agreement
- **e.** Welcome to the Optivity Telephony Manager Setup
- **f.** Identification
- **g.** Setup Choices

3 Enter the serial number and keycode of the OTM package you want to install. See Figure 37 on page 91. Click **Next** to continue.

Figure 37
Enter Keycodes dialog box



Enter Keycodes

Enter the serial number details and keycode for the software packages.

Serial Number: OTM12345

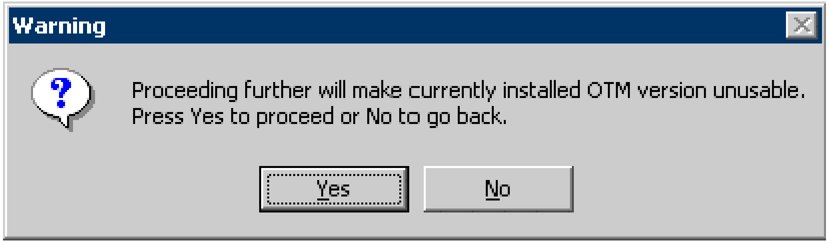
Licensed to: Admin

Keycode: H4XE

Note: Previous OTM keycodes do not work. You must use the OTM keycode for the new package.

The Warning message appears. See Figure 38.

Figure 38
Warning message



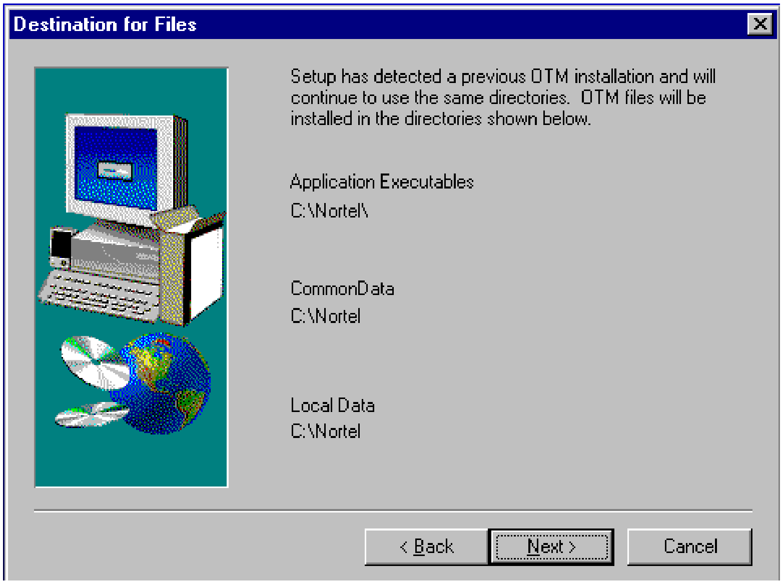
Warning

Proceeding further will make currently installed OTM version unusable. Press Yes to proceed or No to go back.

4 Click **Yes** to continue.

The Destination for Files dialog box appears. The directory path of the previously selected Application files, Common Data files, and Local Data files are shown. See Figure 39 on page 92.

Figure 39
Destination for Files dialog box



Destination for Files

Setup has detected a previous OTM installation and will continue to use the same directories. OTM files will be installed in the directories shown below.

Application Executables
C:\Nortel\

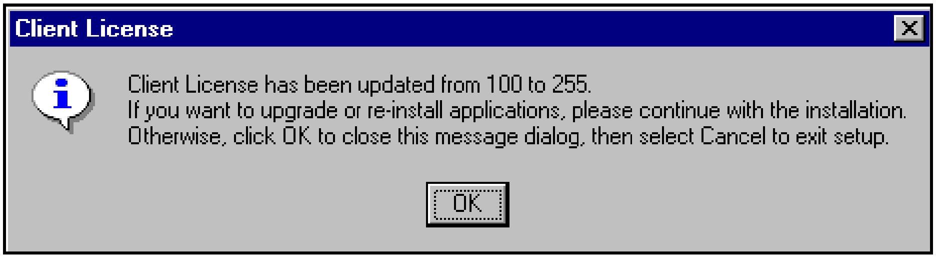
CommonData
C:\Nortel

Local Data
C:\Nortel

5 Click **Next** to continue.

The client License message box appears. See Figure 40.

Figure 40
client License message box



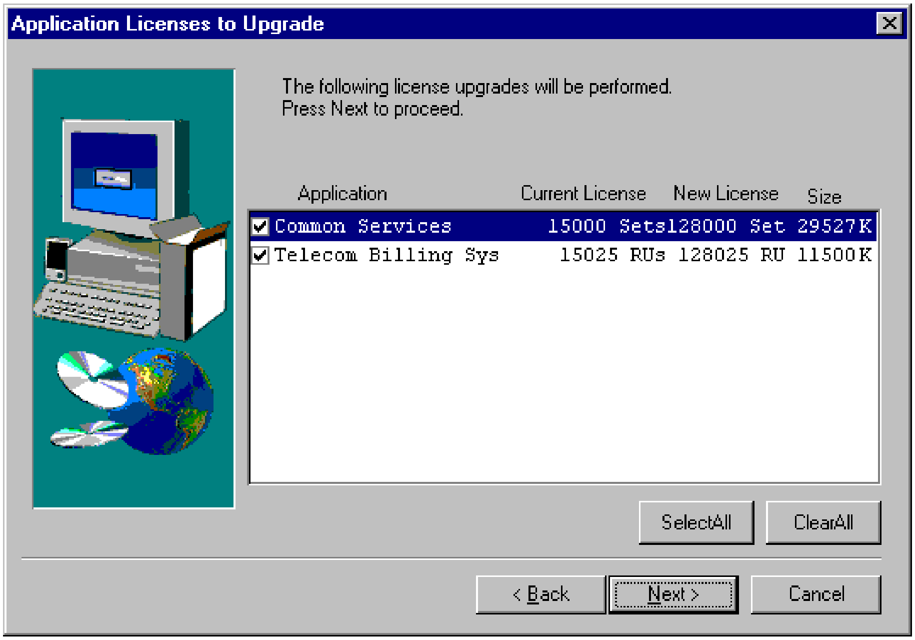
Client License

Client License has been updated from 100 to 255.
If you want to upgrade or re-install applications, please continue with the installation.
Otherwise, click OK to close this message dialog, then select Cancel to exit setup.

6 Click **OK** to continue.

The **Application Licenses to Upgrade** dialog box appears. See Figure 41 on page 93. It provides a summary of the license upgrades that will be performed.

Figure 41
Application Licenses to Upgrade



Application Licenses to Upgrade

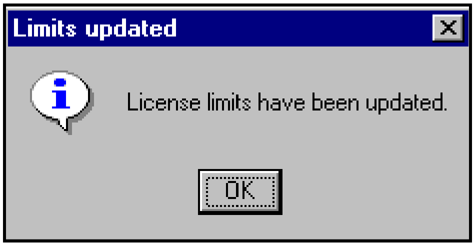
The following license upgrades will be performed.
Press Next to proceed.

Application	Current License	New License	Size
☑ Common Services	15000 Sets	128000 Set	29527K
☑ Telecom Billing Sys	15025 RUs	128025 RU	11500K

7 Click **Next** to continue.

The **Limits updated** message box appears. See Figure 42.

Figure 42
Limits updated message box



Limits updated

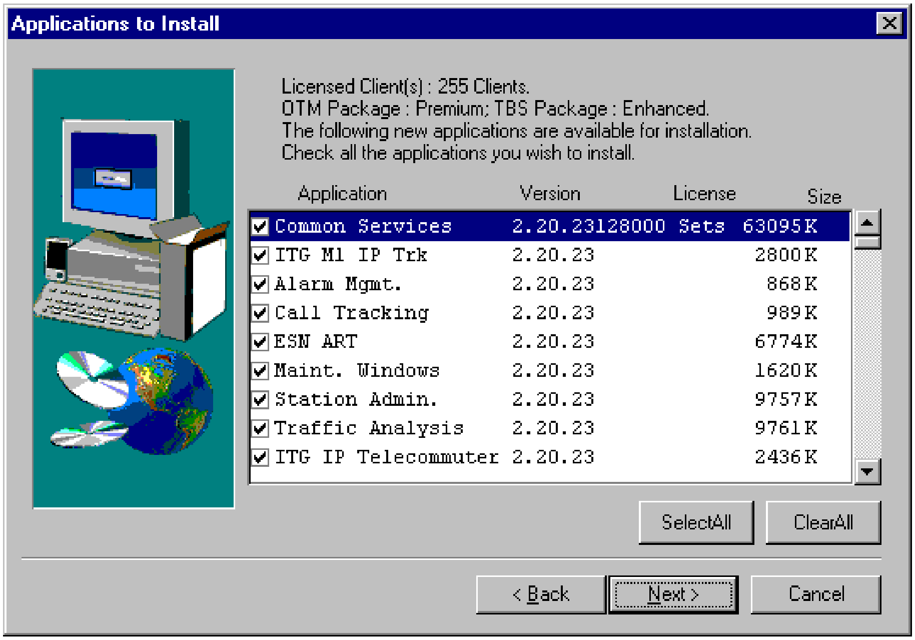
License limits have been updated.

8 Click **OK** to continue. A window dialog box displays a statement that some DLL files are in use and the PC needs to be re-booted.

9 Click **Next** to continue.

The list of applications which were not selected during installation appears. See Figure 43.

Figure 43
Applications to Install dialog box



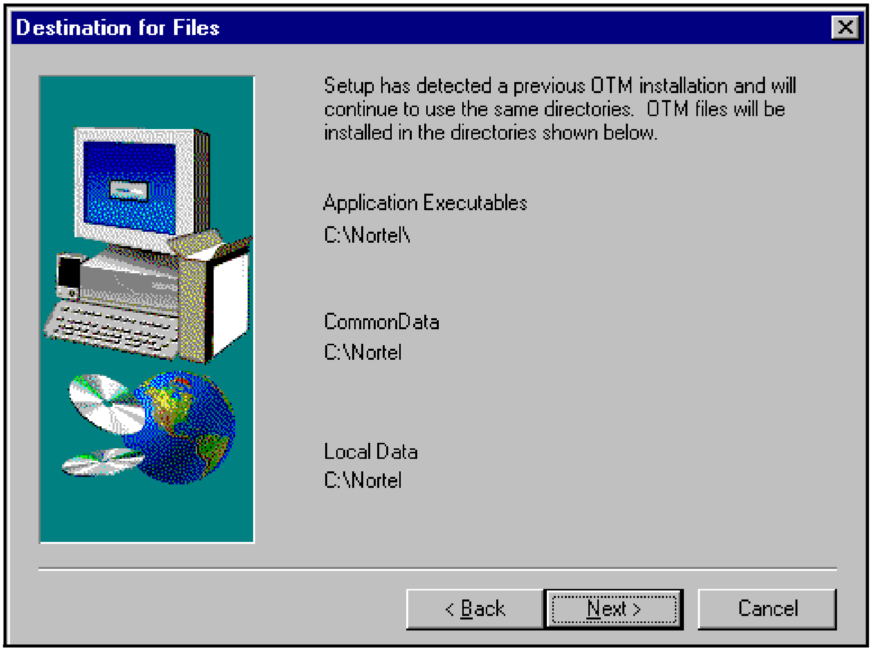
Licensed Client(s) : 255 Clients.
OTM Package : Premium; TBS Package : Enhanced.
The following new applications are available for installation.
Check all the applications you wish to install.

Application	Version	License	Size
☑ Common Services	2.20.23	128000 Sets	63095K
☑ ITG M1 IP Trk	2.20.23		2800K
☑ Alarm Mgmt.	2.20.23		868K
☑ Call Tracking	2.20.23		989K
☑ ESN ART	2.20.23		6774K
☑ Maint. Windows	2.20.23		1620K
☑ Station Admin.	2.20.23		9757K
☑ Traffic Analysis	2.20.23		9761K
☑ ITG IP Telecommuter	2.20.23		2436K

10 Select the applications you need to add.

The **Applications to Re-install** dialog box appears. See Figure 44 on page 95.

Figure 44
Applications to Re-Install



Destination for Files

Setup has detected a previous OTM installation and will continue to use the same directories. OTM files will be installed in the directories shown below.

Application Executables
C:\Nortel\

CommonData
C:\Nortel

Local Data
C:\Nortel

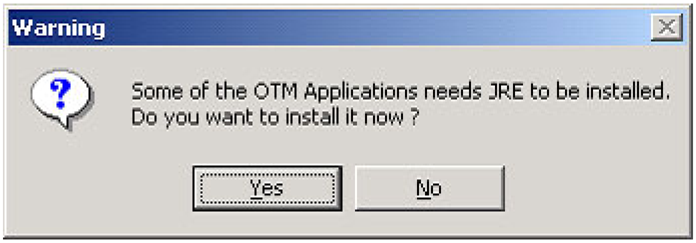
11 Make any modifications to the selected applications. All the check boxes are selected by default. Clearing any check box uninstalls that particular application.

12 Click **Next** to continue.

A Read Me dialog box prompts you to read the readme.txt file. Click **Yes** to view the Read Me file or **No** to skip the Read Me file.

13 If you have installed applications that require Java* Runtime Environment (JRE), you are prompted to install JRE at this point. See Figure 45 on page 96. Click **Yes** if you want to install JRE now. JRE is required for the Alarm Script Wizard and the DECT application.

Figure 45
JRE Installation



Warning

Some of the OTM Applications needs JRE to be installed.
Do you want to install it now ?

You may decide to install JRE at a later time. The JRE install program is located in the OTM directory (for example, C:\Nortel) at:

- For Windows: *C:\Nortel\OMServices\Jre\Windows\j2re-1_4_2-win.exe*
- For other operating systems: Support for Java Plug-in Software on other operating systems is provided by the operating system vendor. For more information on Java Plug-in documentation and Frequently Asked Questions, refer to
  http://java.sun.com/.

JRE is required for the Alarm Script Wizard and the DECT application. After clicking **Yes**, a **Limits Updated** window appears asking you to restart your computer after the JRE installation is completed.

14 Click **OK** to continue.

The Java 2 Runtime Environment installShield Wizard for Java 2 appears.

15 Click **Next** to continue. The **Program Maintenance** window appears.

16 Select **Modify** to modify previously installed JAVA applications .

17 Click **Next.** The **Custom Setup** window appears.

18 Click on **Next t**o continue.The Progress window appears where Java is being installed.

19 Click **Finish** to complete installation.

20 Restart the computer. A dialog box asks you to restart the computer or end the installation without restarting the computer. Select **Yes**, **I want to restart my computer now**, and then click **OK** to continue. After reboot, the Database upgrade utility runs automatically.

> **Note**
>
> To avoid mis-alignment of pages when printing multiple pages of designation strips in station administration, please perform the following steps.
>
> **1**. After installation/upgrade of OTM, uninstall the "Generic/Text only" printer.
>
> **2.** Reboot the PC.
>
> **3.** Re-install the "Generic/Text only" printer.
>
> **4**. Reboot the PC.

End of Procedure

Amending TN licenses or Reporting Units

Procedure 6
Amending TN licenses or Reporting Units

If an upgrade is done on a server in a client server setup, close all OTM client applications and OTM server applications, then reboot the server.

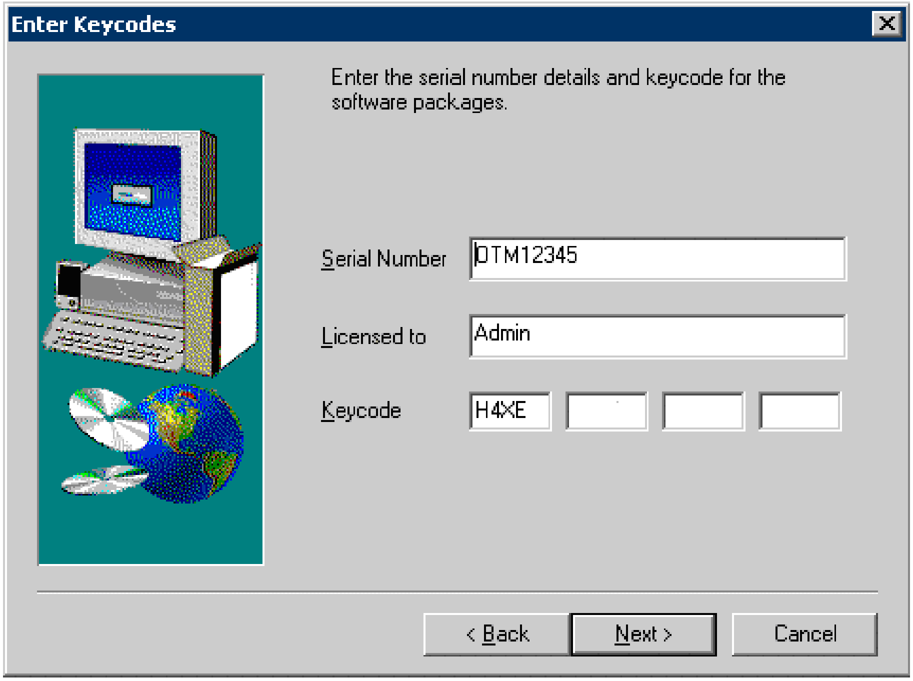
1 Double-click *Setup.exe* on the OTM CD-ROM.

2 Navigate through the OTM installation wizard. The following screens appear (see “Installing OTM software” on page 53).

- **a.** Welcome to the Software Installation Wizard
- **b.** Software selection
- **c.** Software selection confirmation
- **d.** OTM Software Licences Agreement
- **e.** Welcome to the Optivity Telephony Manager Setup
- **f.** Identification
- **g.** Setup Choices

3 Enter the serial number and keycode that you received with your OTM software package in the Enter Keycodes dialog box. see Figure 46 on page 98. Click **Next** to continue.

Figure 46
Enter Keycodes dialog box



Enter Keycodes

Enter the serial number details and keycode for the software packages.

Serial Number: OTM12345

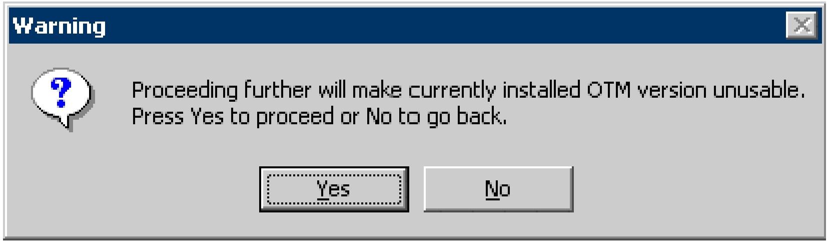
Licensed to: Admin

Keycode: H4XE

> ***Note:*** Previous OTM keycodes do not work. You must use the new OTM keycode.

The Warning message appears. See Figure 47.

Figure 47
Warning message



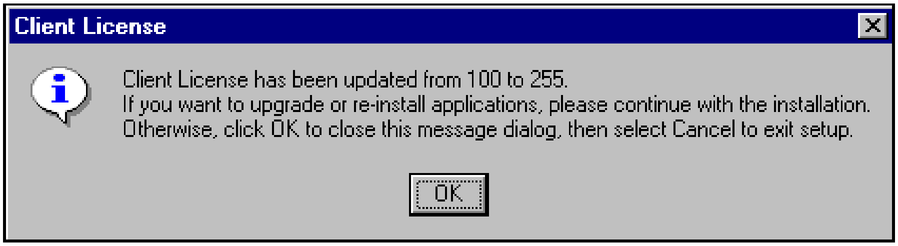
Warning

Proceeding further will make currently installed OTM version unusable. Press Yes to proceed or No to go back.

4 Click **Yes** to continue.

The client License message box appears. See Figure 48 on page 99.

Figure 48
client License message box

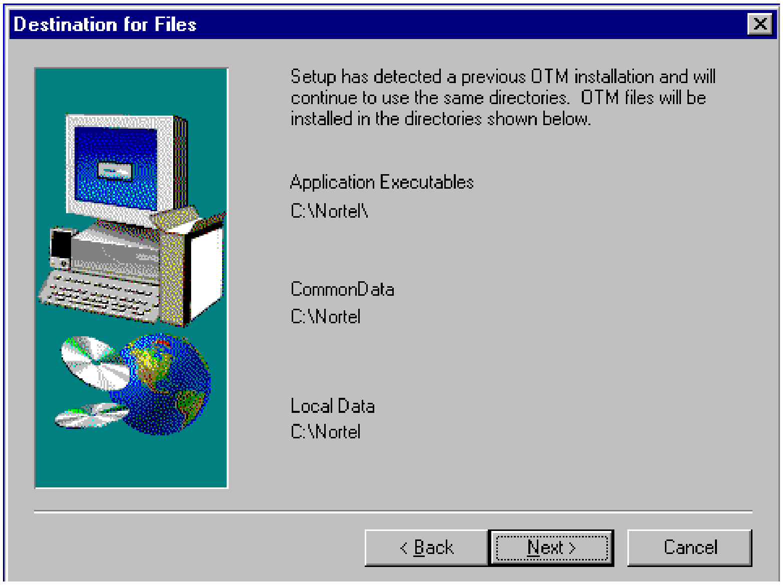


Client License

Client License has been updated from 100 to 255.
If you want to upgrade or re-install applications, please continue with the installation.
Otherwise, click OK to close this message dialog, then select Cancel to exit setup.

5 Click **OK**. The **Destination for Files** dialog box appears. The directory path of the previously selected Application files, Common Data files, and Local Data files) are shown. See Figure 39 on page 92.

Figure 49
Destination for Files dialog box



Destination for Files

Setup has detected a previous OTM installation and will continue to use the same directories. OTM files will be installed in the directories shown below.

Application Executables
C:\Nortel\

CommonData
C:\Nortel

Local Data
C:\Nortel

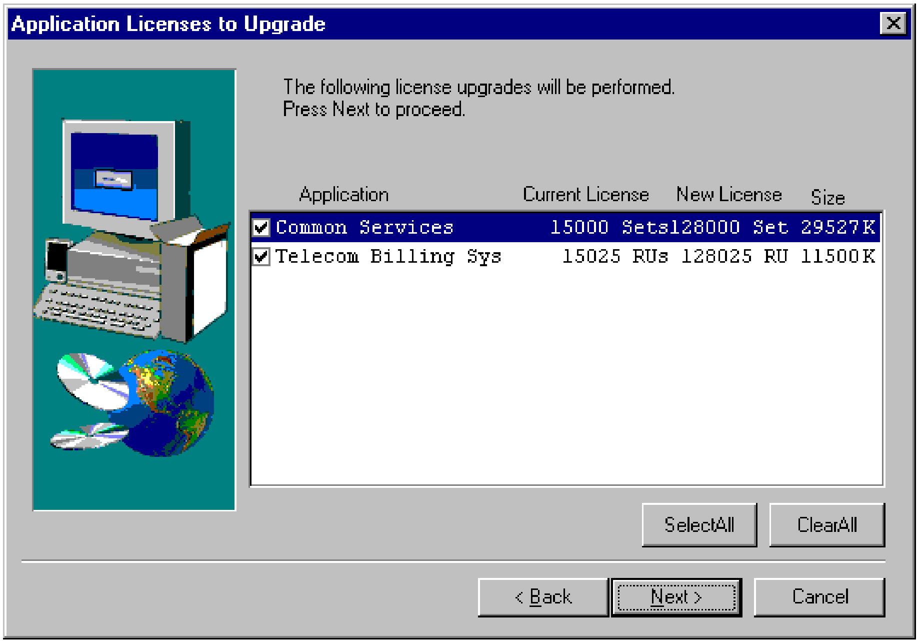
6 Click **Next** to continue.

The Application Licenses to Upgrade dialog box appears. See Figure 50. It provides a summary of the license upgrades that will be performed.

CAUTION — Service Interruption

Do not select Cancel to exit setup as indicated in Figure 49 on page 99, if you want the licenses to be completely updated. Selecting Cancel updates client licenses only . Set licenses are not updated at this point.

Figure 50
Application Licenses to Upgrade



Application Licenses to Upgrade

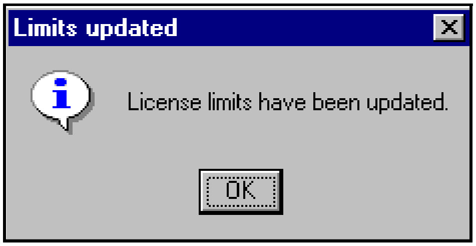
The following license upgrades will be performed.
Press Next to proceed.

Application	Current License	New License	Size
☑ Common Services	15000 Sets	128000 Set	29527K
☑ Telecom Billing Sys	15025 RUs	128025 RU	11500K

7 Click **Next** to continue.

The Limits updated message box appears.

Figure 51
Limits updated message box



Limits updated

License limits have been updated.

8 Click **OK** to continue.

The license limits have all been successfully updated at this point.

9 If there are no further updates required to the OTM installation, click **Cancel** at the next screen to exit the setup.

If there are further updates required to the OTM installation, continue with steps 8 to 16 of "Upgrading to another OTM package" on page 90.

End of Procedure

Upgrading the OTM client software

Upgrade the OTM client software for the following reasons:

- to upgrade OTM applications not previously installed
- to upgrade to another OTM package

Upgrading to OTM applications not previously installed

This situation occurs when the OTM server is upgraded. The OTM client does not require an upgrade unless the client needs to access the ugraded applications.

Upgrading to another OTM package

This situation occurs if the OTM server is upgraded to another OTM package (for example, the keycode is changed), then the OTM client must also be upgraded. Follow the procedure .

Procedure 7
Upgrading the OTM client software

1 Double-click *S***etup.exe** on the OTM CD-ROM.The OTM installation wizard appears.

2 Navigate through the OTM installation wizard. The following screens appear (see "Installing OTM software" on page 53).

a. Welcome to the Software Installation Wizard

b. Software selection

c. Software selection confirmation

d. OTM Software Licences Agreement

e. Welcome to the Optivity Telephony Manager Setup

f. Identification

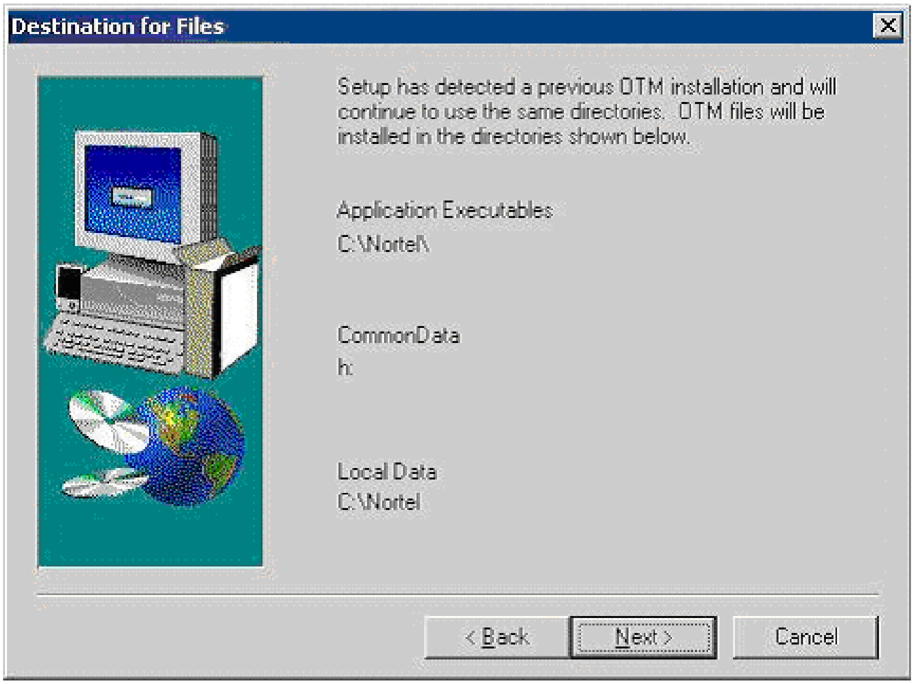
g. Setup Choices

Note: If required and not present on the PC, the setup program installs DCOM at this point. Once installed, you must reboot the PC. After you reboot and log in, the OTM software installation continues.

3 In the Setup Choices dialog box, select client, then click **Next**.

The **Destination for files** dialog box appears. See Figure 52 on page 103. The Destination for files dialog box shows the directory path of Application Executables, Common Data, and Local Data. This is where the OTM files were stored in the original installation, and where the new files will be stored.

Figure 52
Destination for files dialog box



Destination for Files

Setup has detected a previous OTM installation and will continue to use the same directories. OTM files will be installed in the directories shown below.

Application Executables
C:\Nortel\

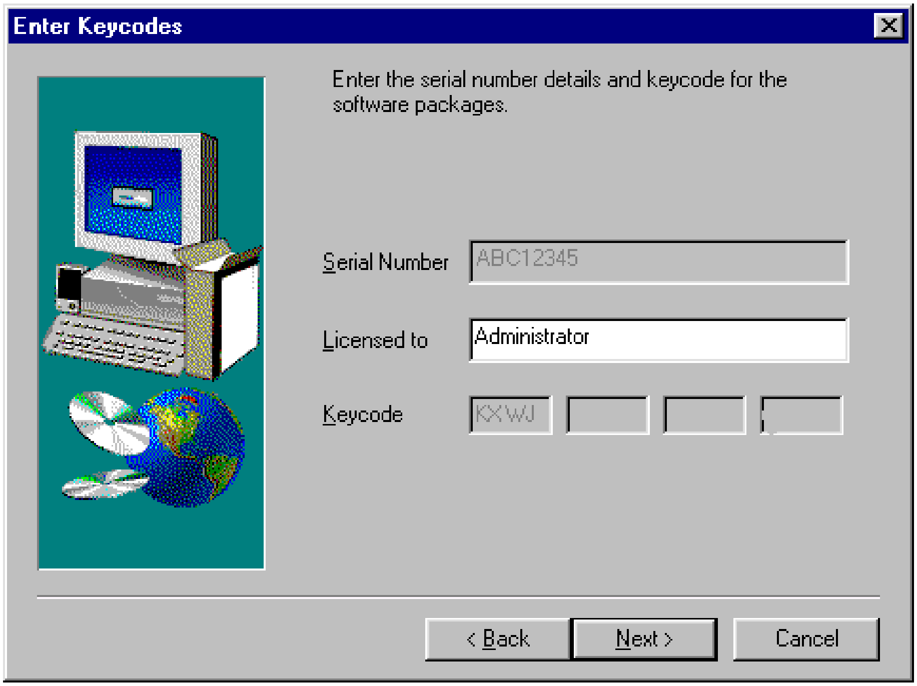
CommonData
h:

Local Data
C:\Nortel

4 Click **Next** to continue.

The **Enter Keycodes** dialog box appears. See Figure 53 on page 104. The fields contain the data stored on the OTM server.

Figure 53
Enter Keycodes dialog box



Enter Keycodes

Enter the serial number details and keycode for the software packages.

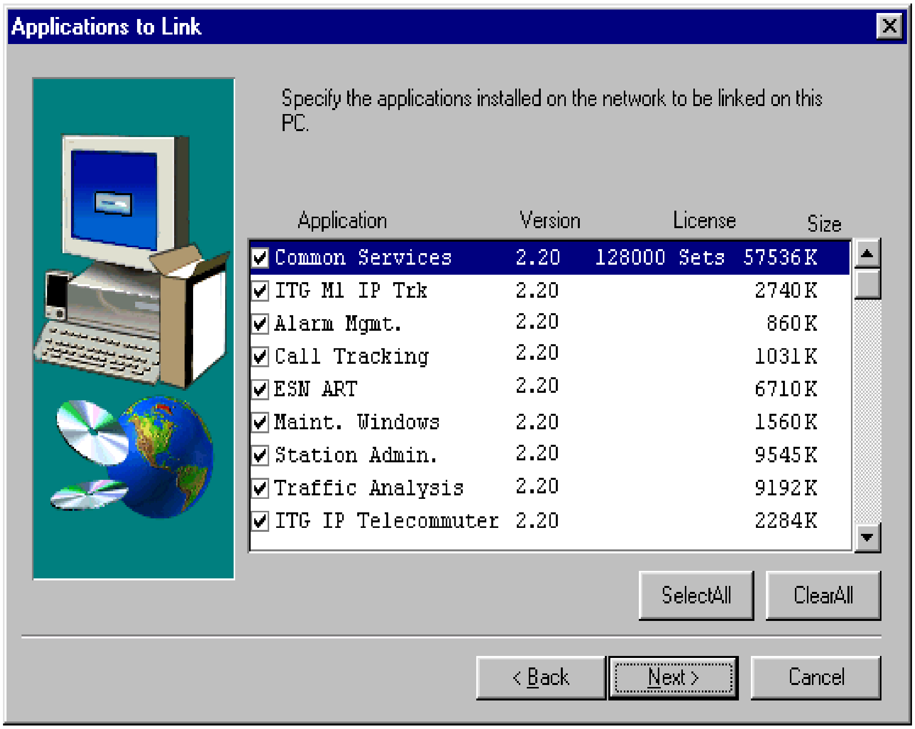
Serial Number: ABC12345

Licensed to: Administrator

Keycode: KXWJ

5 Click **Next** to continue. The **Applications to link** window appears. See Figure 54 on page 105.

Figure 54
Applications to Link window



Applications to Link

Specify the applications installed on the network to be linked on this PC.

	Application	Version	License	Size
☑	Common Services	2.20	128000 Sets	57536K
☑	ITG M1 IP Trk	2.20		2740K
☑	Alarm Mgmt.	2.20		860K
☑	Call Tracking	2.20		1031K
☑	ESN ART	2.20		6710K
☑	Maint. Windows	2.20		1560K
☑	Station Admin.	2.20		9545K
☑	Traffic Analysis	2.20		9192K
☑	ITG IP Telecommuter	2.20		2284K

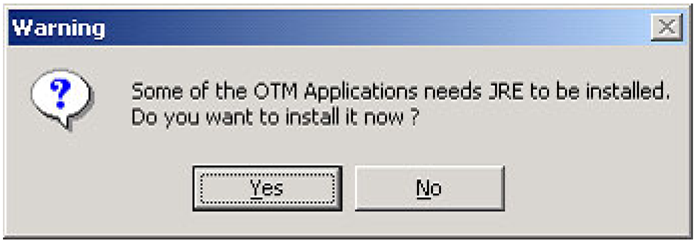
6 Select the required applications to install, then click **Next** to continue. A warning appears “Proceeding further will make the currently installed OTM version unusable”

The installation begins.

7 After the installation is complete, you are given the option to view the Read Me file. Click **Yes** to view the Read Me file or **No** to skip the Read Me file.

8 If you have installed applications that require Java* Runtime Environment (JRE), you are prompted to install JRE at this point. See Figure 55 on page 106. Click **Yes** if you want to install JRE now. JRE is required for the Alarm Script Wizard and the DECT application.

Figure 55
JRE Installation



Warning

Some of the OTM Applications needs JRE to be installed.
Do you want to install it now ?

You may decide to install JRE at a later time. The JRE install program is located in the OTM directory (for example, C:\Nortel) at:

- For Windows: *C:\Nortel\OMServices\Jre\Windows\j2re-1_4_2-win.exe*
- For other operating systems: Support for Java Plug-in Software on other operating systems is provided by the operating system vendor. For more information on Java Plug-in documentation and Frequently Asked Questions, refer to
  http://java.sun.com/.

JRE is required for the Alarm Script Wizard and the DECT application. After clicking yes, a “Limits Updated” window appears asking you to restart your computer after the JRE installation is completed.

9 Click **OK** to continue.

The Java 2 Runtime Environment installShield Wizard for Java 2 appears.

10 Click **Next** to continue. The **Program Maintenance** window appears.

11 Select **Modify** to modifypreviously installed JAVA applications .

12 Click **Next.** The **Custom Setup** window appears.

13 Click on **Next t**o continue.The **Progress** window appears where Java is being installed.

14 Click **Finish** to complete installation.

15 Restart the computer. A dialog box asks you to restart the computer or end the installation without restarting the computer. Select **Yes**, **I want to restart my computer now**, and then click **OK** to continue. After reboot, the Database upgrade utility runs automatically.

End of Procedure

Performing migrations

Contents

This chapter contains information on the following topics:

Migrating from OTM 1.2/2.0x/2.1 to OTM 2.2

IMPORTANT!

Direct upgrades are NOT supported for customers migrating from OTM releases prior to 1.20.26. A two-step upgrade is required, first to OTM 2.0 or 2.01 and then to 2.2.

Upgrade from MAT pre-6.67 to OTM 2.2 is purchased new and done as a new install.

Upgrade from MAT 6.67 to OTM 2.2 is done as a new install through an upgrade code.

OtmOsMigrate utility paths

This utility does not support OTM Windows® client Migration. Table 10 shows the migration paths supported by this utility.

Table 10
Migration paths (Part 1 of 2)

From	To
OTM 1.2/2.0x on WinNT 4.0 Workstation	OTM 2.2 on Win2000 Pro
OTM 1.2/2.0x on WinNT 4.0 Workstation	OTM 2.2 on WinXP Pro
OTM 1.2/2.0x on WinNT 4.0 server	OTM 2.2 on Windows 2000 server

Table 10
Migration paths (Part 2 of 2)

From	To
OTM 2.1 on WinNT 4.0 server	OTM 2.2 on Windows 2000 server
OTM 2.1 on WinNT 4.0 Workstation	OTM 2.2 on Win2000 Pro/WinXP Pro
OTM 2.1 on Win2000 Pro	OTM 2.2 on Win2000 Pro
OTM 2.1 on Win2000 Pro	OTM 2.2 on WinXP Pro
OTM 2.1 on WinXP Pro	OTM 2.2 on Win2000 Pro
OTM 2.1 on WinXP Pro	OTM 2.2 on WinXP Pro

Procedure 8
Migrating from OTM 1.2/2.0x/2.1 to OTM 2.2

1 Back up files on existing OTM. If migrating to a new OS or a new PC, then use the OtmOsMigrate tool described in the following section.

2 If migrating to a new OS or a new PC, then:

  a. Prepare the new PC.

  b. Use the OtmOsMigrate tool described in the following section to restore the existing version of OTM onto new PC. No OTM dongle is required for this step.

3 Install OTM 2.2 onto the PC. This migrates the existing OTM data from OTM 1.2/2.0x/2.1 to OTM 2.2. A valid OTM 2.2 keycode must be entered during this step. If changing dongle types and the new dongle has a different serial number, then it also requires a different keycode. If changing dongles, enter the keycode for the new dongle which is to be connected in the next step.

4 Ensure the dongle is connected to the PC. If migrating from a parallel port to USB dongle, switch dongles now.

  Note: USB dongles can only be used with OTM 2.1 or OTM 2.2.

5 Launch OTM 2.2.

End of Procedure

Upgrading Windows NT server to Windows 2000 server

IMPORTANT!

Before migrating, go to **OTM Navigator > Maintenance > Event log viewer > Tools > SNMP Trap settings** and ensure that the **Lock Properties** checkbox is unchecked in the **Trap Settings** dialog box.

Procedure 9

WARNING

Back up the Alarm Notification control and script files separately. The script files may be replaced during a software upgrade.

Upgrading Windows NT server to Windows 2000 server

Complete the following steps to migrate OTM 1.2/2.0x/2.1 installed on Windows NT server to OTM 2.2 on Windows 2000 using the OtmOsUpgrade Utility.

1 Back up the OTM files on Windows NT server to another location.

From the Command Line window, execute the following:

```
OtmOsUpgrade -backup directoryPath [-batch]
```

This copies all the OTM information from the Windows NT server machine to the directoryPath. The directoryPath can be a shared folder on the network to which the user has read/write access rights to.

2 Restore OTM onto the new Windows 2000 server.

From the new Windows 2000 server machine, execute the following command:

```
OtmOsUpgrade -restore directoryPath [-batch]
```

This restores all the OTM information from the specified directoryPath.

3 Install OTM 2.2.

Install OTM 2.2 on the Windows 2000 server machine. The installation program detects the restored OTM information and implements the proper migration procedures.

IMPORTANT!

After migration, OTM 2.2 must be installed in exactly the same location as the previous OTM version. For example, if OTM 1.2/2.0x/2.1 is installed on “c:\Nortel” on Window NT server, after migrating to Windows 2000 server, OTM 2.2 must be installed in the same location on “c:\Nortel”.

End of Procedure

Windows client migration

The OtmOsUpgrade utility does not support OTM Windows client Migration since all the common data resides on the OTM Windows server. After upgrading the OTM Windows server, OTM 2.2 Windows client can be installed on any new PC.

Local user account on new PC

The OTM user account from the local Windows NT account database cannot be migrated. This limitation applies to OTM 2.0x/2.1 installed on Windows NT server. OTM does not store the user password. Users are required to recreate the local user account on the new PC. Once those local accounts (with the same name) are recreated, the OTM user /group relationship remains intact. There is no need to recreate local user groups.

Upgrading Windows NT/98 PC to Windows XP Pro/2000 Pro PC

The procedure, “Upgrading Windows 98/NT 4.0 to Windows XP/2000 Pro” on page 111, creates a “Dummy OTM“ on a Windows XP Pro/Windows 2000 Pro machine. It appears to the installation program that there is an old OTM version installed. This triggers the correct migration/upgrade logic. The utility backs up the installed OTM on the Windows 98/Windows NT 4.0 Workstation, including executable, DLLs, data and registry, and restores them to the same location on a Windows XP Pro/ Windows 2000 Pro PC.

Upgrading Windows 98/NT 4.0 to Windows XP/2000 Pro

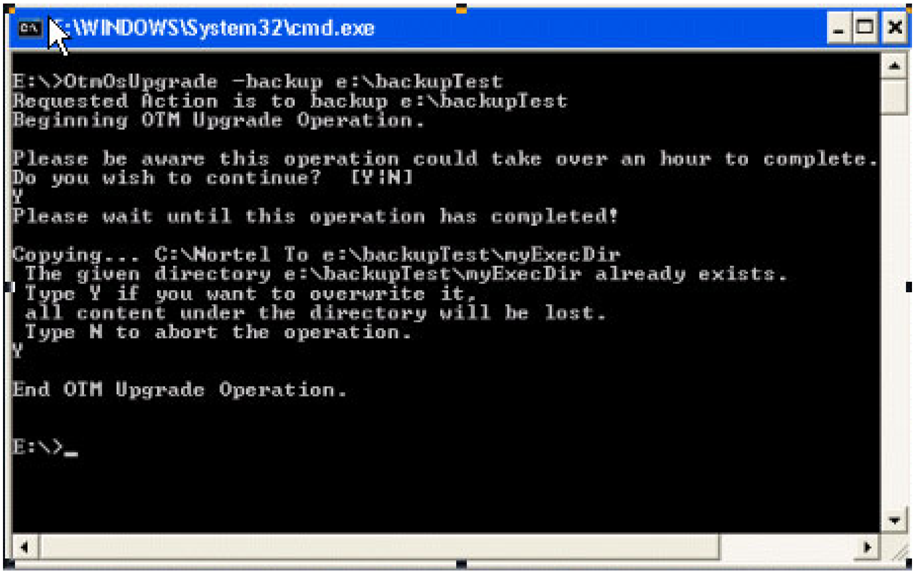
With OTM installed on a Windows NT 4.0 Workstation, the OTM user account from the local Windows NT account database cannot be migrated. OTM does not store the user password. You must re-create the local user account on the new PC. Once those local accounts (with the same name) are re-created, the OTM user template relationship stays untouched. There is no need to recreate local user groups for each template.

Procedure 10
Upgrading Windows 98/NT 4.0 to Windows XP/2000 Pro

To move old OTM data from one PC running Win98/WinNT 4.0 Workstation to another PC running WinXP Pro/Win2000 Pro, complete the following steps.

1 On the Win98/WinNT 4.0 Workstation machine, use the “-backup directoryPath [-batch]” option to back up all the OTM information. See Figure 56. The directoryPath can be a shared folder to which you have read/write access.

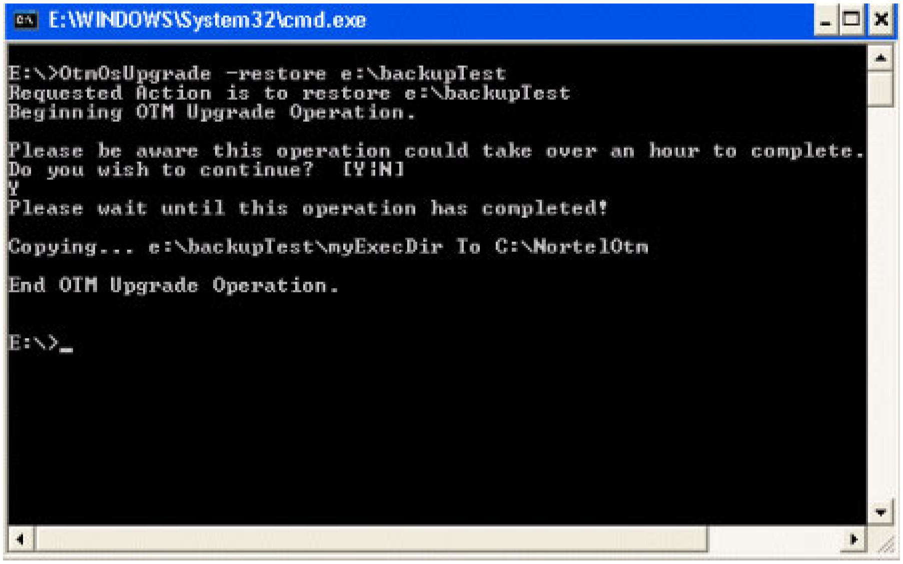
Figure 56
Back up option



```
E:\>OtmOsUpgrade -backup e:\backupTest
Requested Action is to backup e:\backupTest
Beginning OTM Upgrade Operation.

Please be aware this operation could take over an hour to complete.
Do you wish to continue?  [Y|N]
Y
Please wait until this operation has completed!

Copying... C:\Nortel To e:\backupTest\myExecDir
 The given directory e:\backupTest\myExecDir already exists.
 Type Y if you want to overwrite it.
 all content under the directory will be lost.
 Type N to abort the operation.
Y

End OTM Upgrade Operation.


E:\>_
```

2 On the WinXP Pro/Win2000 Pro machine, use the “-restore directoryPath [-batch]” option to restore all the OTM information from directoryPath. See Figure 57.

Figure 57
Restore option



```
E:\>OtmOsUpgrade -restore e:\backupTest
Requested Action is to restore e:\backupTest
Beginning OTM Upgrade Operation.

Please be aware this operation could take over an hour to complete.
Do you wish to continue?  [Y|N]
Y
Please wait until this operation has completed!

Copying... e:\backupTest\myExecDir To C:\NortelOtm

End OTM Upgrade Operation.


E:\>_
```

3 Install OTM 2.2 on the WinXP Pro/Win2000 Pro machine. The installation program detects the OTM 2.01 information and implements proper migration.

After migration, OTM 2.2 must be installed on exactly the same location as the old OTM version. For example, if an OTM 2.01 is installed on “c:\Nortel” on a Windows NT 4.0 Workstation, after migrating to WinXP Pro, OTM 2.2 must be installed on the same location “c:\Nortel”.

4 Using the OtmOsUpgrade utility, back up directoryPath [-batch]. Back up all the OTM directories and OTM-related registry information into the destinationPath. If -batch is given, no user input is required.

The OtmOsUpgrade utility is a CLI-based script written in Jscript and running inside Windows Script Host. The earliest version of Windows Script Host required by this utility is 2.0. IE 6 or later must be installed on the PC before running the OtmOsUpgrade utility.

5 Restore directoryPath [-batch], restore the OTM registry information, and restore OTM directories from directoryPath to the proper target location. If -batch is given, no user input is required.

End of Procedure

OTM Web Help

Contents

This chapter contains information on the following topics:

Overview

This chapter contains information on installing Web Help.

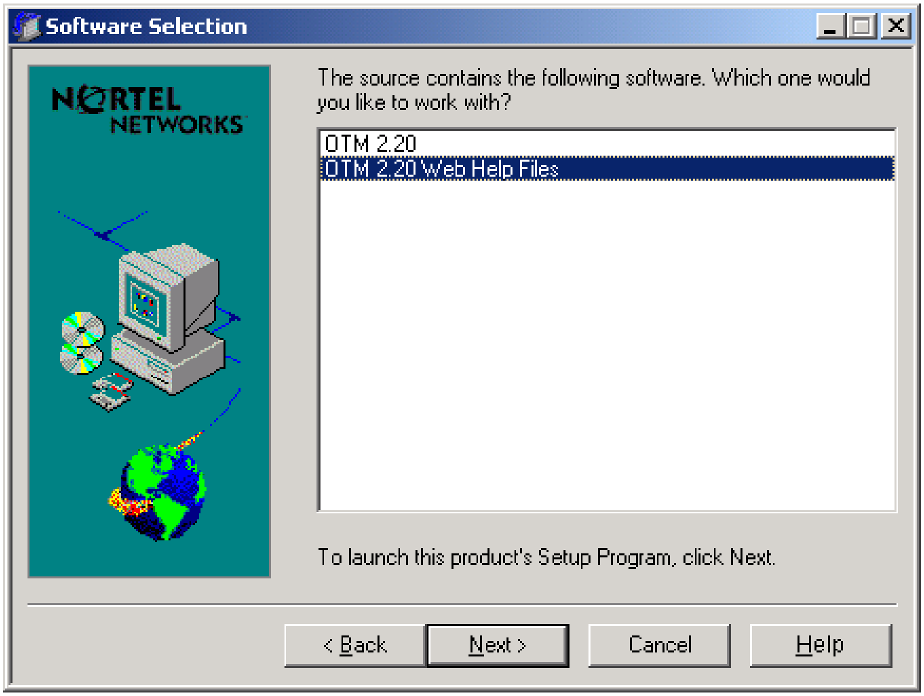
If you will be using OTM web Services, install the web-based Help files by selecting the option in the Software Selection dialog box. See Figure 58 on page 114.

Installing Web Help

Procedure 11
Installing Web Help

1. Double-click the **Setup.exe** file to launch the Software Installation Wizard . See Figure 1 on page 54. Click **Next** to continue.
2. Select **OTM 2.20 Web Help Files**, and then click **Next.** See Figure 58 on page 114.

Figure 58
Software Selection: Web Help



Software Selection

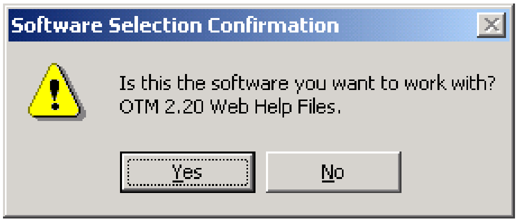
The source contains the following software. Which one would you like to work with?

OTM 2.20
OTM 2.20 Web Help Files

To launch this product's Setup Program, click Next.

The **Software Selection Confirmation** dialog box, see Figure 59, opens to request confirmation that OTM 2.2 Web Help Files is the software that you want to work with.

Figure 59
Confirmation Dialog Box



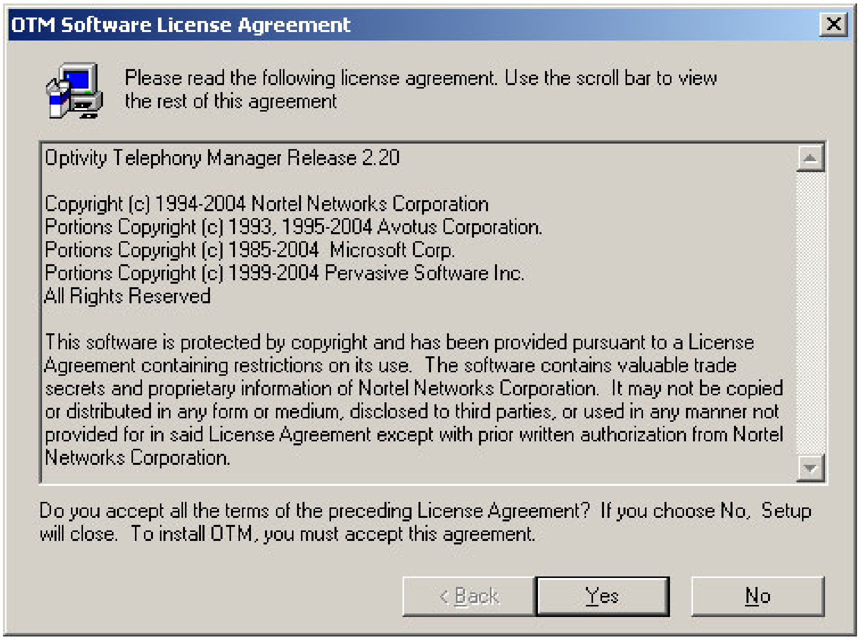
Software Selection Confirmation

Is this the software you want to work with?
OTM 2.20 Web Help Files.

3 Click **Yes** to continue.

4 The **Software License Agreement** is the first dialog box displayed when you launch the OTM installation program. See Figure 60 on page 115. Click **Yes** to accept the agreement.

Figure 60
Help License



OTM Software License Agreement

Please read the following license agreement. Use the scroll bar to view the rest of this agreement

Optivity Telephony Manager Release 2.20

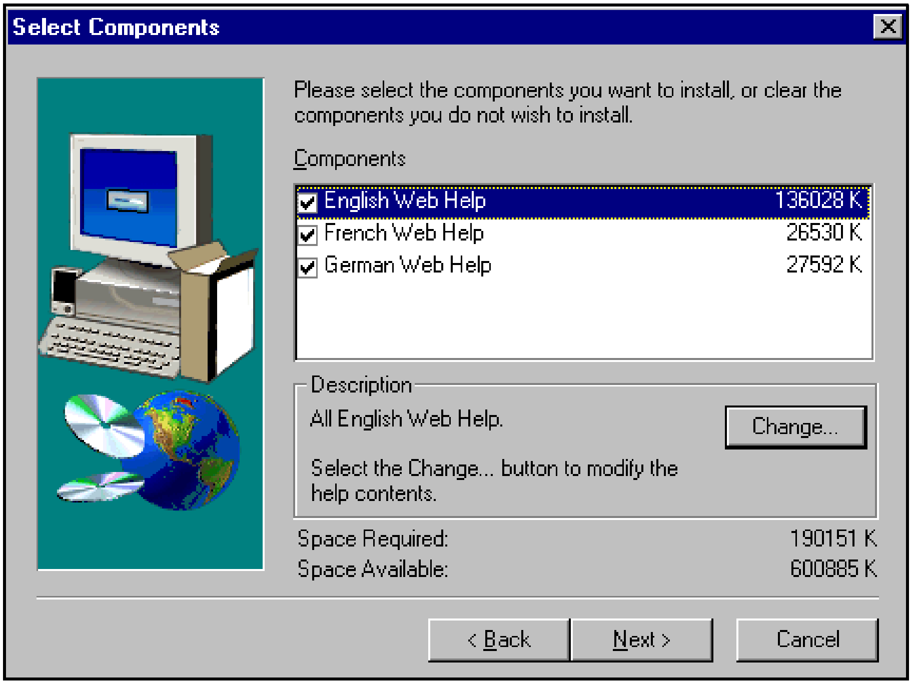
Copyright (c) 1994-2004 Nortel Networks Corporation
Portions Copyright (c) 1993, 1995-2004 Avotus Corporation.
Portions Copyright (c) 1985-2004 Microsoft Corp.
Portions Copyright (c) 1999-2004 Pervasive Software Inc.
All Rights Reserved

This software is protected by copyright and has been provided pursuant to a License Agreement containing restrictions on its use. The software contains valuable trade secrets and proprietary information of Nortel Networks Corporation. It may not be copied or distributed in any form or medium, disclosed to third parties, or used in any manner not provided for in said License Agreement except with prior written authorization from Nortel Networks Corporation.

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install OTM, you must accept this agreement.

The **Select Components** dialog box appears. See Figure 61 on page 116.

Figure 61
Select Web Help components dialog box



Select Components

Please select the components you want to install, or clear the components you do not wish to install.

Components

☑ English Web Help	136028 K
☑ French Web Help	26530 K
☑ German Web Help	27592 K

Description

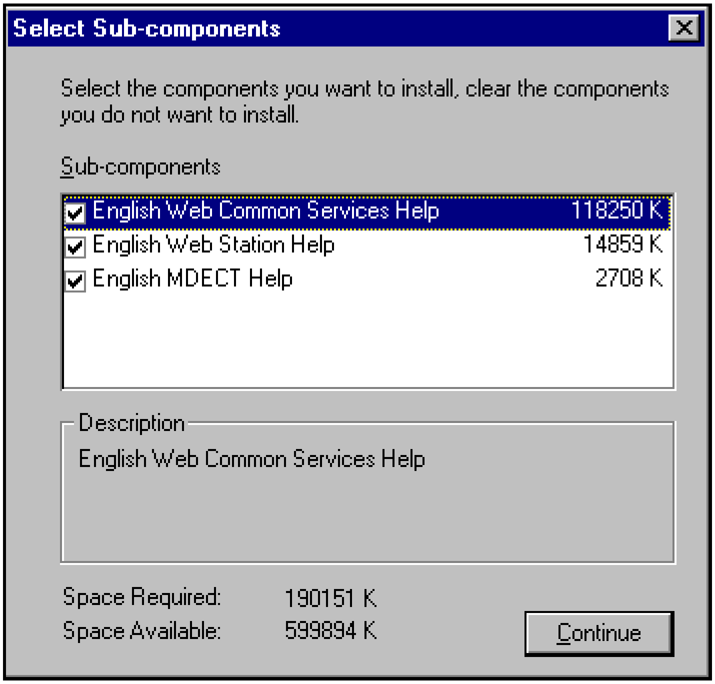
All English Web Help.

Select the Change... button to modify the help contents.

Space Required:	190151 K
Space Available:	600885 K

5 In the **Select Components** dialog box, click **Next** to install all English, French, and German helpfiles by default, or click **Change** to select the sub-components that you want to install. See Figure 62 on page 117.

Figure 62
Select Sub-components dialog box



Select Sub-components

Select the components you want to install, clear the components you do not want to install.

Sub-components

☑	English Web Common Services Help	118250 K
☑	English Web Station Help	14859 K
☑	English MDECT Help	2708 K

Description
English Web Common Services Help

Space Required: 190151 K
Space Available: 599894 K

6 Click **Continue** in the **Select Sub-components** dialog box, see Figure 62, to return to the Select Components dialog box (Figure 61 on page 116).

7 Click **Next** to start the Web Help installation process.

8 When the installation is completed, the **Web Help installation** complete window appears. Click **OK**.

End of Procedure

Microsoft IIS Lockdown wizard

The following steps describe the recommended configuration settings of the IIS Security Tool when installed on an OTM server. Any settings that differ from the recommended configuration may result in the disabling of OTM web applications.

Overview

The IIS Lockdown Wizard is used to configure and install the IIS Security Tool. To change the configuration settings, run the Wizard again.

The default template provided by Microsoft for a dynamic server is used with one exception; the option "Writing to content directories" must be left unchecked.

On installing the Tool, two files (Urlscan.dll and Urlscan.ini) are created.

- The URLScan.dll file is a filter that is self-registered when installed through the IIS Lockdown Wizard. It can be manually registered through the Internet Service Manager interface as well. It pre-processes all requests to the IIS server looking for input as defined in the URLScan.ini configuration file.
- URLScan.ini file has two main parts: option and implementation. The option part of this file allows the user to enable or disable a particular option while the later supports the actual configuration of the enabled option. This file can be edited manually by the user to change the options.

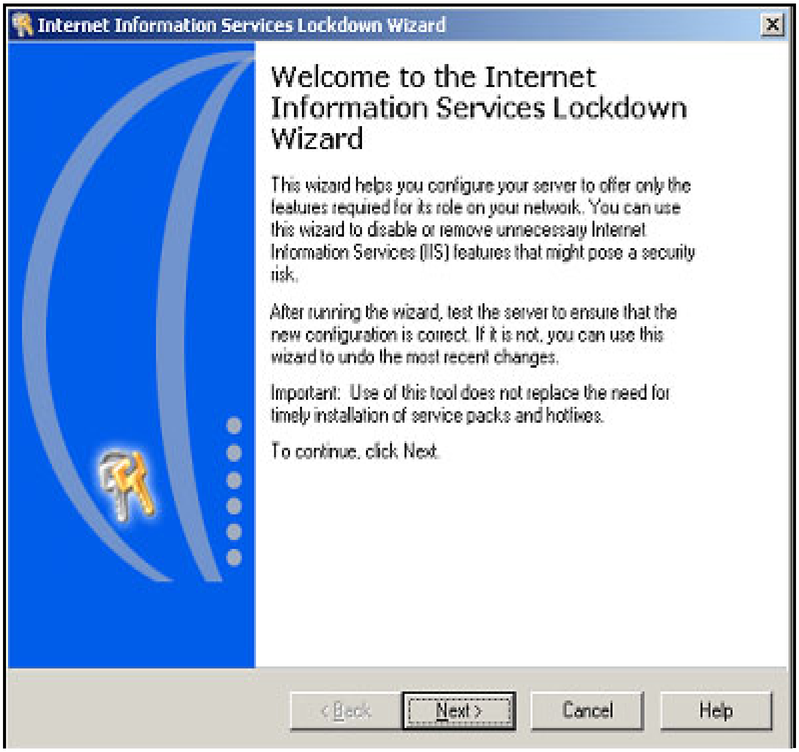
Note: Manual changes to the two files created by the IIS Lockdown Wizard may result in the disabling of OTM web applications.

Procedure 12
Configuring the IIS Lockdown wizard

1 Download the iislock.exe from Microsoft and save to your desktop.

2 To run the wizard, click **iislockd.exe**. The Welcome window appears. See Figure 63. Click **Next.** The **License agreement** window appears. See Figure 64 on page 121.

Figure 63
IIS-Welcome



Internet Information Services Lockdown Wizard

Welcome to the Internet Information Services Lockdown Wizard

This wizard helps you configure your server to offer only the features required for its role on your network. You can use this wizard to disable or remove unnecessary Internet Information Services (IIS) features that might pose a security risk.

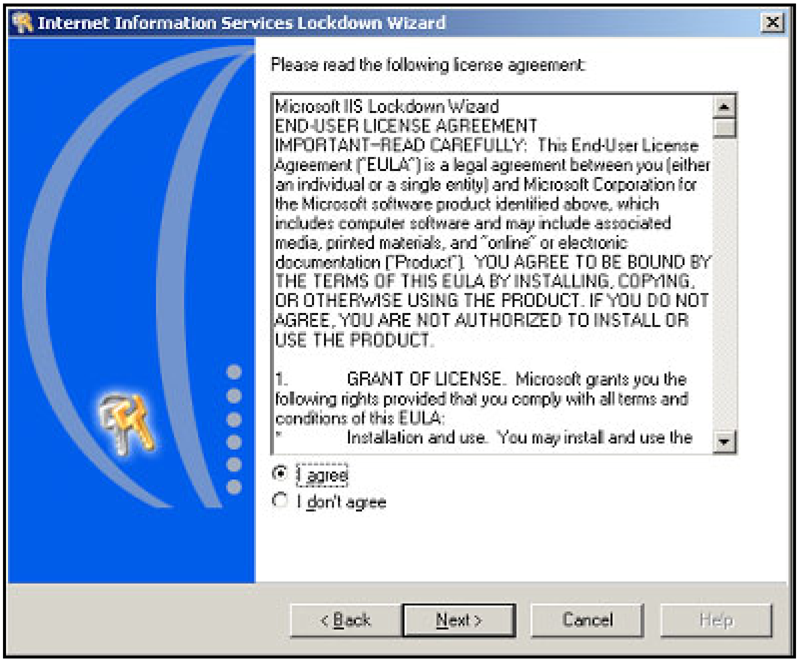
After running the wizard, test the server to ensure that the new configuration is correct. If it is not, you can use this wizard to undo the most recent changes.

Important: Use of this tool does not replace the need for timely installation of service packs and hotfixes.

To continue, click Next.

3 Select **I agree**. Click **Next**. The **Select Server Template** window appears. See Figure 65 on page 122.

Figure 64
License agreement



Please read the following license agreement:

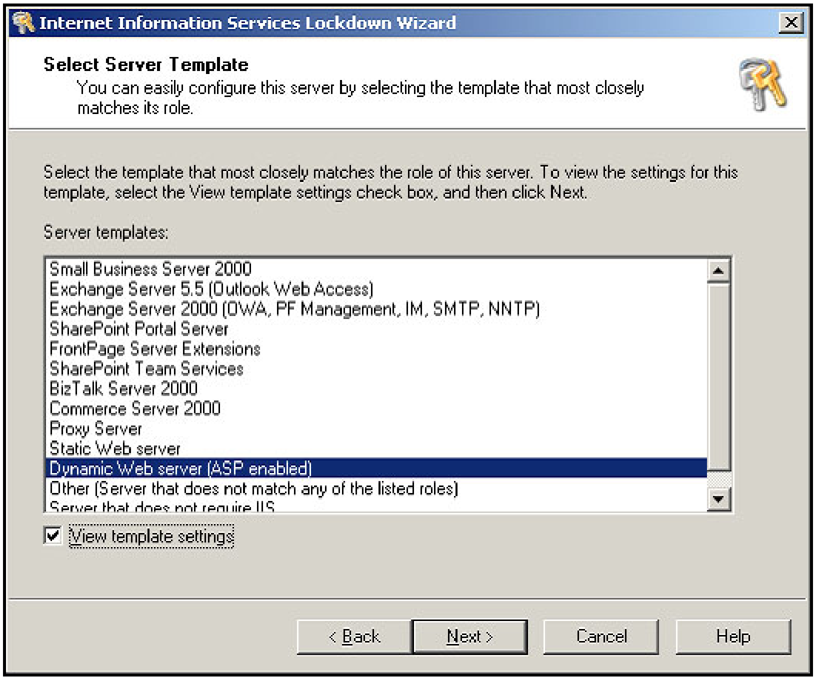
Microsoft IIS Lockdown Wizard
END-USER LICENSE AGREEMENT
IMPORTANT–READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation for the Microsoft software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("Product"). YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR OTHERWISE USING THE PRODUCT. IF YOU DO NOT AGREE, YOU ARE NOT AUTHORIZED TO INSTALL OR USE THE PRODUCT.

1. GRANT OF LICENSE. Microsoft grants you the following rights provided that you comply with all terms and conditions of this EULA:
* Installation and use. You may install and use the

● I agree
○ I don't agree

4 Select the server Template **Dynamic web server (ASP enabled)** and enable the checkbox **View template settings**. Click **Next**. The I**nternet Services** window appears. See Figure 66 on page 123.

Figure 65
Select server template



Internet Information Services Lockdown Wizard

Select Server Template

You can easily configure this server by selecting the template that most closely matches its role.

Select the template that most closely matches the role of this server. To view the settings for this template, select the View template settings check box, and then click Next.

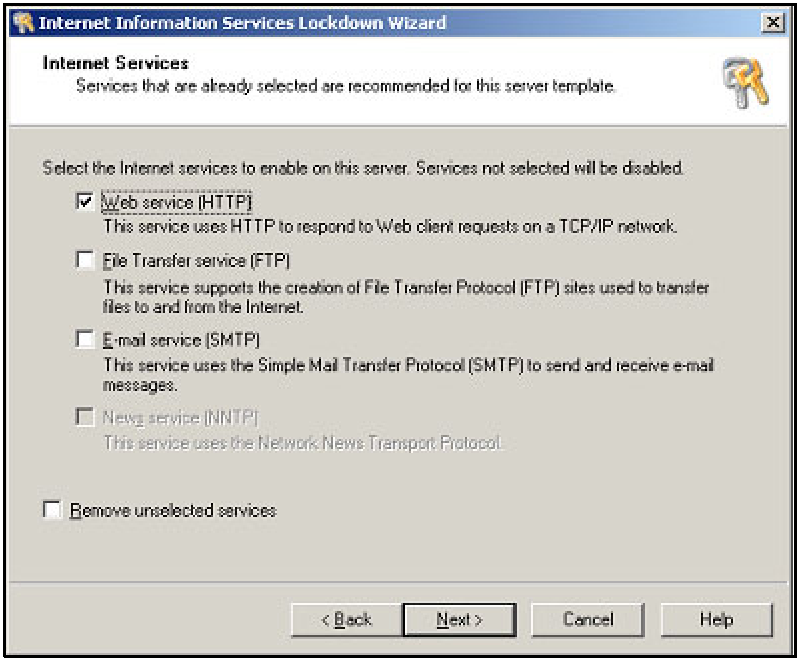
Server templates:

- Small Business Server 2000
- Exchange Server 5.5 (Outlook Web Access)
- Exchange Server 2000 (OWA, PF Management, IM, SMTP, NNTP)
- SharePoint Portal Server
- FrontPage Server Extensions
- SharePoint Team Services
- BizTalk Server 2000
- Commerce Server 2000
- Proxy Server
- Static Web server
- Dynamic Web server (ASP enabled)
- Other (Server that does not match any of the listed roles)
- Server that does not require IIS

☑ View template settings

5 Keep the defaults settings (only **Web service (HTTP)** is enabled). Click **Next**. The **Script Maps** window appears. See Figure 67 on page 124.

Figure 66
Internet Services



Internet Information Services Lockdown Wizard

Internet Services

Services that are already selected are recommended for this server template.

Select the Internet services to enable on this server. Services not selected will be disabled.

☑ Web service (HTTP)
This service uses HTTP to respond to Web client requests on a TCP/IP network.

□ File Transfer service (FTP)
This service supports the creation of File Transfer Protocol (FTP) sites used to transfer files to and from the Internet.

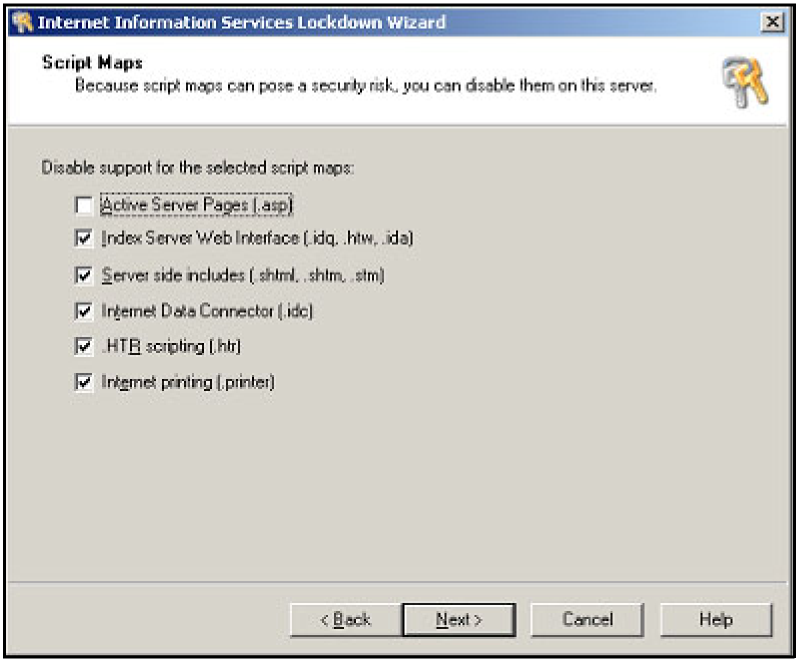
□ E-mail service (SMTP)
This service uses the Simple Mail Transfer Protocol (SMTP) to send and receive e-mail messages.

□ News service (NNTP)
This service uses the Network News Transport Protocol.

□ Remove unselected services

6 Keep the default settings (**Active server pages (.asp)** is enabled). Click **Next**. The **Additional Security** window appears. See Figure 68 on page 125.

Figure 67
Script Maps



Internet Information Services Lockdown Wizard

Script Maps

Because script maps can pose a security risk, you can disable them on this server.

Disable support for the selected script maps:

☐ Active Server Pages (.asp)

☑ Index Server Web Interface (.idq, .htw, .ida)

☑ Server side includes (.shtml, .shtm, .stm)

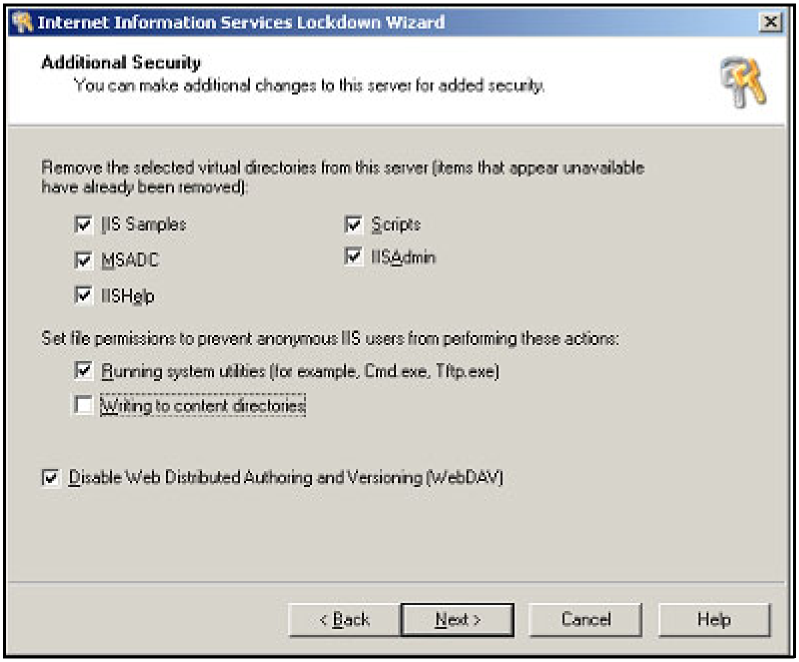
☑ Internet Data Connector (.idc)

☑ .HTR scripting (.htr)

☑ Internet printing (.printer)

7 Deselect **Writing to content directories** checkbox. Keep all other default settings. Click **Next**. The **URLScan** window appears. See Figure 69 on page 126.

Figure 68
Additional security



Internet Information Services Lockdown Wizard

Additional Security

You can make additional changes to this server for added security.

Remove the selected virtual directories from this server (items that appear unavailable have already been removed):

☑ IIS Samples ☑ Scripts

☑ MSADC ☑ IISAdmin

☑ IISHelp

Set file permissions to prevent anonymous IIS users from performing these actions:

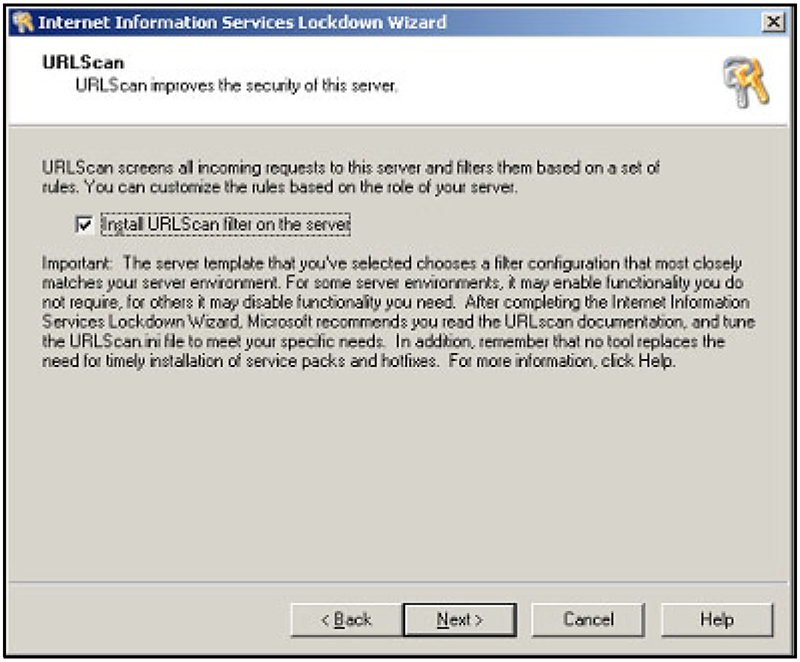
☑ Running system utilities (for example, Cmd.exe, Tftp.exe)

□ Writing to content directories

☑ Disable Web Distributed Authoring and Versioning (WebDAV)

8 Select **Install URLScan filter on the server checkbox**. Click **Next**. The **Ready to Apply** window appears. See Figure 70 on page 127.

Figure 69
URLScan



URLScan

URLScan improves the security of this server.

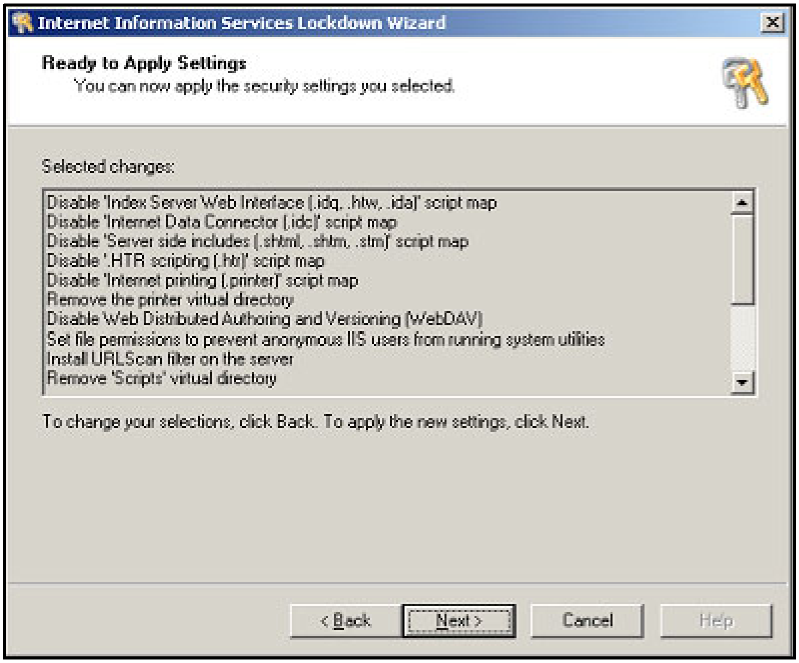
URLScan screens all incoming requests to this server and filters them based on a set of rules. You can customize the rules based on the role of your server.

☑ Install URLScan filter on the server

Important: The server template that you've selected chooses a filter configuration that most closely matches your server environment. For some server environments, it may enable functionality you do not require, for others it may disable functionality you need. After completing the Internet Information Services Lockdown Wizard, Microsoft recommends you read the URLscan documentation, and tune the URLScan.ini file to meet your specific needs. In addition, remember that no tool replaces the need for timely installation of service packs and hotfixes. For more information, click Help.

9 Click **Next.** The **Applying to Security Settings window appears. See** Figure 71 on page 128.

Figure 70
Ready to apply



Ready to Apply Settings

You can now apply the security settings you selected.

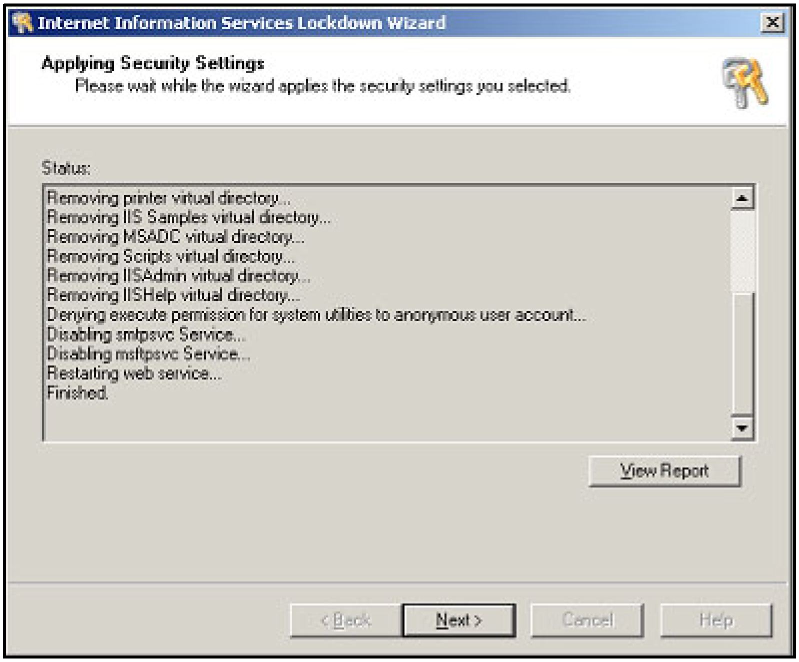
Selected changes:

Disable 'Index Server Web Interface (.idq, .htw, .ida)' script map
Disable 'Internet Data Connector (.idc)' script map
Disable 'Server side includes (.shtml, .shtm, .stm)' script map
Disable '.HTR scripting (.htr)' script map
Disable 'Internet printing (.printer)' script map
Remove the printer virtual directory
Disable Web Distributed Authoring and Versioning (WebDAV)
Set file permissions to prevent anonymous IIS users from running system utilities
Install URLScan filter on the server
Remove 'Scripts' virtual directory

To change your selections, click Back. To apply the new settings, click Next.

10 Click **Next**. The **Completing IIS Lockdown** window appears. See Figure 72 on page 129.

Figure 71
Applying to security settings



Applying Security Settings

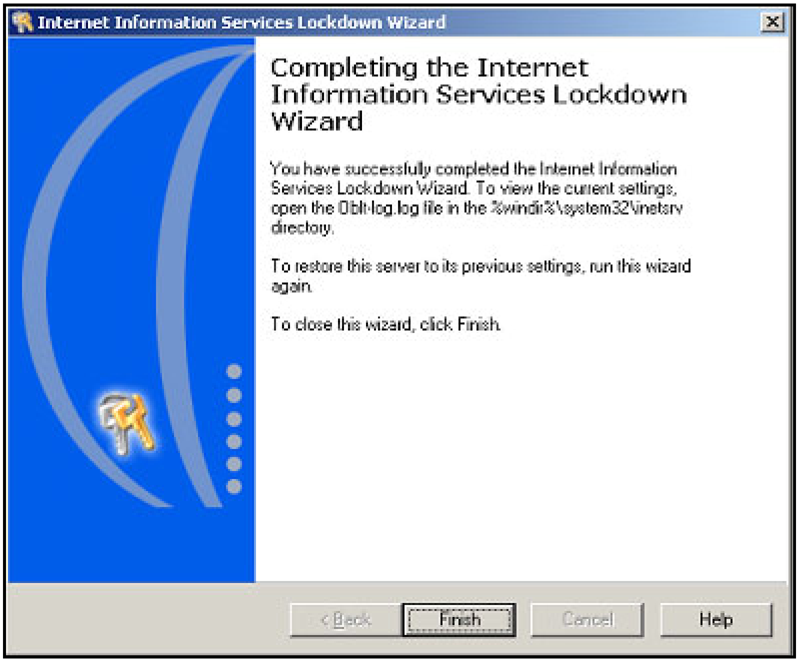
Please wait while the wizard applies the security settings you selected.

Status:

```
Removing printer virtual directory...
Removing IIS Samples virtual directory...
Removing MSADC virtual directory...
Removing Scripts virtual directory...
Removing IISAdmin virtual directory...
Removing IISHelp virtual directory...
Denying execute permission for system utilities to anonymous user account...
Disabling smtpsvc Service...
Disabling msftpsvc Service...
Restarting web service...
Finished.
```

11 Click **Finish**. The window closes.

Figure 72
Completing IIS Lockdown



Completing the Internet Information Services Lockdown Wizard

You have successfully completed the Internet Information Services Lockdown Wizard. To view the current settings, open the Oblt-log.log file in the %windir%\system32\inetsrv directory.

To restore this server to its previous settings, run this wizard again.

To close this wizard, click Finish.

End of Procedure

Adding the default user created by IIS ie " IUSR_<computer name> " to the Administrators group prevents errrors.

Procedure 13
Adding IIS default user name to Administrator’s group

1 Go to **Computer Management > Local Users and Groups.**

2 Note that a default user "IUSR_<computer_name>" is already present.

3 Right- click and select **Properties**, select **Member Of** tab. If this user is not member of Administrator groups, add Administrator Groups to this user.

End of Procedure

Configuring Secure Sockets Layer (SSL)

Contents

This section contains information on the following topics:

Overview

To use Secure Sockets Layer (SSL) in web applications, a server certificate must be installed in Internet Information Services (IIS). For the certificate to become valid, the key-storage file which contains both private and public keys and is password- protected must be used. Private and public keys are used by the browser and IIS to negotiate encryption.

SSL client authentication on Sun One 5.2 directory server

IMPORTANT!

OTM does not support client authentication using x.509 certificate. If the Sun One LDAP server enables the client authentication, the open LDAP client API does not negotiate properly with the 5.2 Sun One server and the error code **error 81, cannot contact server** appears.

Installing a server certificate in IIS

OTM server can be configured to use SSL to protect passwords in network transport during the login sequence. For the SSL transport to become fully operational, an SSL server certificate must be installed in IIS. You can obtain your own server certificate from a trusted authority (for example, Verisign) or generate your own certificate using a certificate server. This document assumes you have already obtained a server certificate and only describes the steps required to install the certificate.

Configuring SSL on the OTM server platform

Procedure 14
Configuring SSL on the OTM server platform

To install the certificate from the Internet Services Manager application on a Windows server, complete the following procedure:

1 Launch the application from **Programs > Administrative Tools > Internet Services Manager**.

2 From the left navigator pane, select the Default website.

3 Right-click on Default website and select **Properties**.

4 From the **Properties** window, select **Directory Security** tab and click **Server Certificate** under Secure Communications. The web server Certificate Wizard then walks you through the installation of the certificate.

5 After the certificate installation has been completed, go to the Default website Properties window and select the web site tab. Ensure the SSL Port is set to 443.

End of Procedure

Enabling SSL for OTM web login

Procedure 15
Enabling SSL for OTM web login

To enable SSL for OTM web login, complete the following procedure.

1 From OTM Navigator (Windows or web), launch the User Authentication application.

2 Select the checkbox **Use SSL for web login authentication**.

End of Procedure

Importing OTM Root Certificate

Enabling SSL for OTM web login may cause long delays before the login page is displayed. When IIS receives an incoming SSL request from a client, it attempts to build its certificate chain before sending its certificate information back to the client. During this time, if the IIS computer does not have the issuing certificate authority's root certificate installed locally, it tries to connect to the certificate authority directly to obtain it. This causes the server to try and resolve the certificate authority's machine name or fully qualified domain name to an IP address.

If the certificate authority (certificate server) is inaccessible from the IIS computer, then IIS continues to resolve the certificate authority's IP address until it times out. These name resolution queries cause SSL connection delays.

To resolve this, the client can import the OTM root certificate into the browser's certificate storage.

To import the OTM root certificate into Internet Explorer certificate storage, complete the following procedure:

Procedure 16
Importing OTM Root Certificate

1. Make the OTM server certificate available to the client PC.
2. From Internet Explorer, select **Tools > Internet Options**.
3. Select **Content** tab and click **Certificates**.
4. Select **Trusted Root Certification Authorities** tab.
5. Click **Import**. The Certificate Import Wizard walks you through the import process.

End of Procedure

Setting up LDAP SSL

Procedure 17
Setting up LDAP SSL

1. Set up Netscape Communicator 4.79 or above, to trust certificate authorities used by LDAP servers that have SSL enabled.

   If the LDAP server certificate is issued by well known certificate authorities such as VeriSign etc., the certificate authority may already be in the Netscape Communicator certificate database by default.

a. Verify the certificate authority is included in Netscape Communicator certificate database. To do this, open the Communicator menu, select **Tools > Security Info**, then click **Signers** on the left side.

b. If the certificate authority is not included in the database, please consult your system administrator for importing a private certificate authority.

2 Locate the certificate database files used by the Netscape Communicator:

a. From C:\Netscape\userName directory (UserName is the current login user name), select **cert7.db**, **key3.db**, and **secmod.db**.

b. Copy the three files to the OTM Common Data directory (usually under c:\Nortel\Common Data).

3 Set up the LDAP SSL connection in OTM server:

a. Open **OTM Windows Navigator**, select **Utilities > LDAP Setup & Logs**.

b. Set the port number to be 636 or the specific SSL port number configured by corresponding LDAP server.

c. Select **Use SSL for authentication and synchronization**.

4 For detailed instructions on setting up the LDAP server, as well as an example of importing attributes to the OTM directory, see LDAP Synchronization in *Optivity Telephony Manager: System Administration* (553-3001-330).

End of Procedure

License management

Contents

This chapter contains information on the following topics:

Serial number and keycode

Keycodes supported on previous releases of OTM do not work in OTM 2.2.

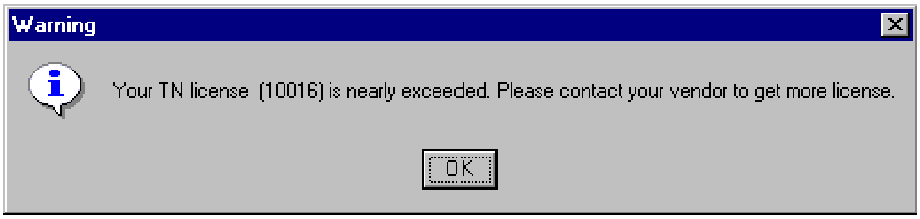
The serial number and keycode you receive with your OTM software package determines the maximum number of terminal numbers (TNs) or telephones, Reporting Units (RUs), and OTM clients that can be configured in your OTM system. To purchase licensing for additional TNs, RUs, or clients, contact your OTM vendor.

TN license

TN license checking

Each time you log in to OTM, your TN license is checked. If the number of set TNs (telephone TNs and virtual TNs) configured in your system is approaching the maximum for your license, the TN **Warning** window appears. See Figure 73 on page 136.

Figure 73
TN license warning

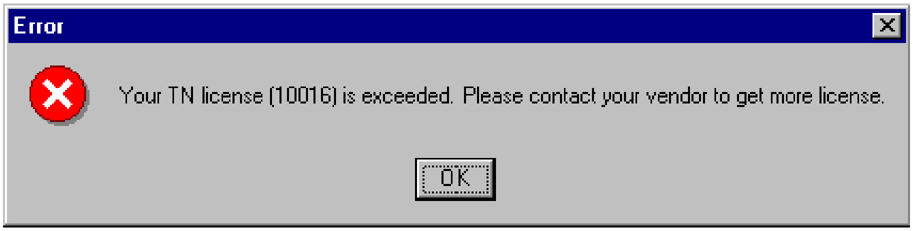


Your TN license (10016) is nearly exceeded. Please contact your vendor to get more license.

License exceeded

If your TN license has been exceeded, an **Error** window appears. See Figure 74. This message appears every 15 minutes. Contact your vendor to obtain a license for additional TNs.

Figure 74
TN license error



Your TN license (10016) is exceeded. Please contact your vendor to get more license.

License reuse

TN checking is performed on bootup and after every 12 hours of operation. If you delete a site, the TN licenses associated with that site becomes available for reuse after the next TN check. If you are unable to wait for the next TN check, you can reboot the OTM server.

RU license

Reporting Units (RUs) are the base used for licensing the telemanagement applications in OTM. An RU represents a single entity in the OTM Corporate databases to which costs/usage can be assigned and reported on through the telemanagement applications. An entity can be either an employee in the Employee database, an external party in the External Parties database, or a role or project in the Roles/Projects database.

Each time you launch a telemanagement application in OTM, your RU license is checked. If the number of RUs configured in your system is approaching the maximum for your license, a warning dialog box appears.

If your RU license has been exceeded, you receive an error message. The TBS application continues to collect data; however, you cannot cost the data and generate reports. The GCAS application launches, but you cannot generate reports. Contact your vendor to obtain a license for additional RUs.

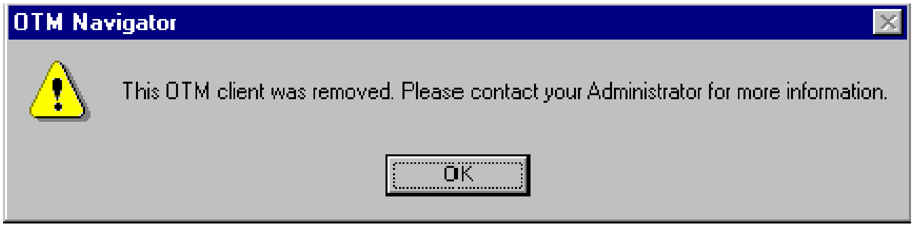
See *Optivity Telephony Manager: Telemanagement Applications* (553-3001-331) for more information.

client license

When you install an OTM client, the host name of the OTM client is registered on the OTM server database. Each time a user attempts to log in to the OTM client, the OTM software checks the OTM database. If the OTM client is not located in the database, the **OTM Navigator** dialog box appears. See Figure 75.

The clients Hostname and IP are saved to the client database. If the IP is changed while the Hostname stays the same then use the client utility.

Figure 75
client removed dialog box



This OTM client was removed. Please contact your Administrator for more information.

The **OTM Navigator** window appears if the OTM client computer's host name has been changed or if the OTM client has been removed from the OTM database.

If the host name of an OTM client computer is changed, the OTM Administrator can use the client Utility to update the host name in the OTM database. For information on the client Utility, refer to *Optivity Telephony Manager: System Administration* (553-3001-330).

Security device (dongle or USB dongle)

Dongle

The process for checking the security device is commonly referred to as the dongle. In OTM, the dongle attached to the OTM server enables access for all of the OTM clients configured on the server.

When OTM is launched from an OTM client, the OTM server's dongle is checked. The OTM client cannot launch the OTM System Window if the OTM server's dongle is missing.

If the dongle has been removed from the OTM server, it takes approximately 5 minutes, once it has been reattached, for the OTM client to recognize the dongle.

> ***Note:*** When a user attempts to log in to Web Navigator after installing OTM for the first time, an error message might display stating that the OTM dongle is missing, when in fact it is not missing. If this occurs, the dongle timer is set to a two-minute interval for dongle checking (instead of the regular 30-minute interval). Therefore, the user must wait a maximum of only two minutes to attempt another Web Navigator login.

USB dongle

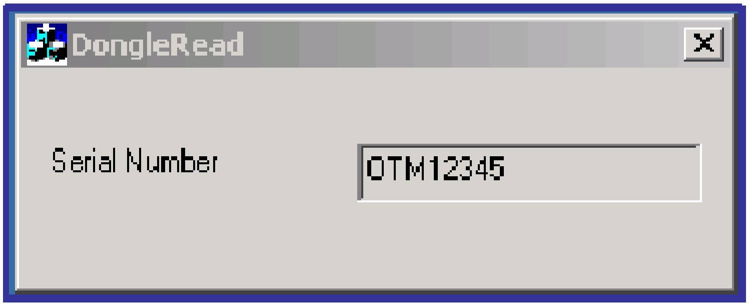
The USB dongle is supported on both the Server and Stand-alone configurations:

- supports one USB dongle only or one parallel port dongle
  - — A dongle connected to a USB port at the same time as one connected to a parallel port is not supported.
  - — Two USB dongles connected at the same time is not supported.
- not supported through a USB hub
  - — USB dongles connected through a USB hub are not supported. USB dongles must be connected to USB ports located on the motherboard or on USB PCI cards.

OTMUtil.exe

OTMUtil.exe is included in the OTM 2.2 Installation CD under the CDINFO folder.When launched, the OTMUtil.exe utility reads the serial number of the dongle attached to the PC and displays it in the **DongleRead** window. See Figure 76. OTM must be installed for the OTMUtil.exe to function.

Figure 76
DongleRead



Serial Number OTM12345

PCI port limitations

PCI-based parallel ports may have problems on certain operating systems. Compaq Proliant DL360R01 running Windows 2000 server using a Lava PCI Bus Enhanced Parallel Port card is one such system. OTM does not support this configuration.

Transfer from parallel port dongle to USB dongle

Migration from a parallel port dongle to USB dongle is supported, as is migration from a USB dongle to a parallel port dongle. To accommodate this, order the transfer code which replaces a parallel port dongle with a USB dongle.

When a customer orders a dongle transfer and goes from a parallel port to USB (or vice versa), the old dongle serial number is no longer valid. The keycode issued is for the new dongle serial number and does not work on the old dongle. The customer is expected to discard the old dongle. This dongle swap or transfer is only for end-user licensed dongles, not for distributor or enterprise licensed dongles. Distributors can just simply order more dongles of either type.

Before configuring OTM

Contents

This chapter contains information on the following topics:

Overview

Before configuring for OTM, test the connection between OTM and your equipment, using the sample site and system configuration. Follow the procedure in this chapter.

After connecting successfully, refer to “Adding a site” in *Optivity Telephony Manager: System Administration* (553-3001-330) to configure your own sites and systems.

The complete list of OTM configuration procedures includes:

- “Configuring Secure Sockets Layer (SSL)” on page 131
- “Configuring a modem for OTM applications” on page 153
- “Initial login” on page 161
- “Testing the connection” on page 142
- “Security Management” on page 163
- “Adding OTM web users” on page 183
- “Setting up the LDAP server” on page 205
- “Configuring the web browser client” on page 213

- "Integrating OTM with Optivity NMS" on page 215
- "Integrating OTM with HP OpenView" on page 233

Testing the connection

Use the following procedures to test the connection between OTM and your equipment. For detailed instructions on adding sites and systems, see "Setting up system data" on page 150.

ELAN subnet required

The Embedded LAN (ELAN) network interface must be configured and devices must be connected to the ELAN subnet before you can test the connection (refer to Appendix A, "Typical configurations" on page 300.

Setting up communications information

Procedure 18
Setting up communications information

1 Double-click **Sample Site** in the OTM Navigator window.

2 Click **Sample System**, and then choose **File > Properties**.

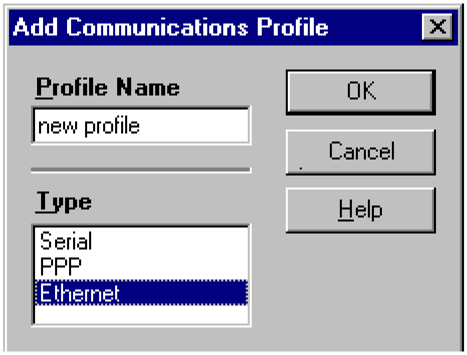
3 The System Properties dialog box appears with the General tab selected.

4 Click **Communications** tab.

5 Click **Add**.

The Add Communications Profile dialog box appears. See Figure 77.

Figure 77
Add Communications Profile dialog box



Add Communications Profile

Profile Name: new profile

Type:
Serial
PPP
Ethernet

6 In the Type box, select a connection type for OTM.

7 Enter a Profile Name.

8 Click **OK**.

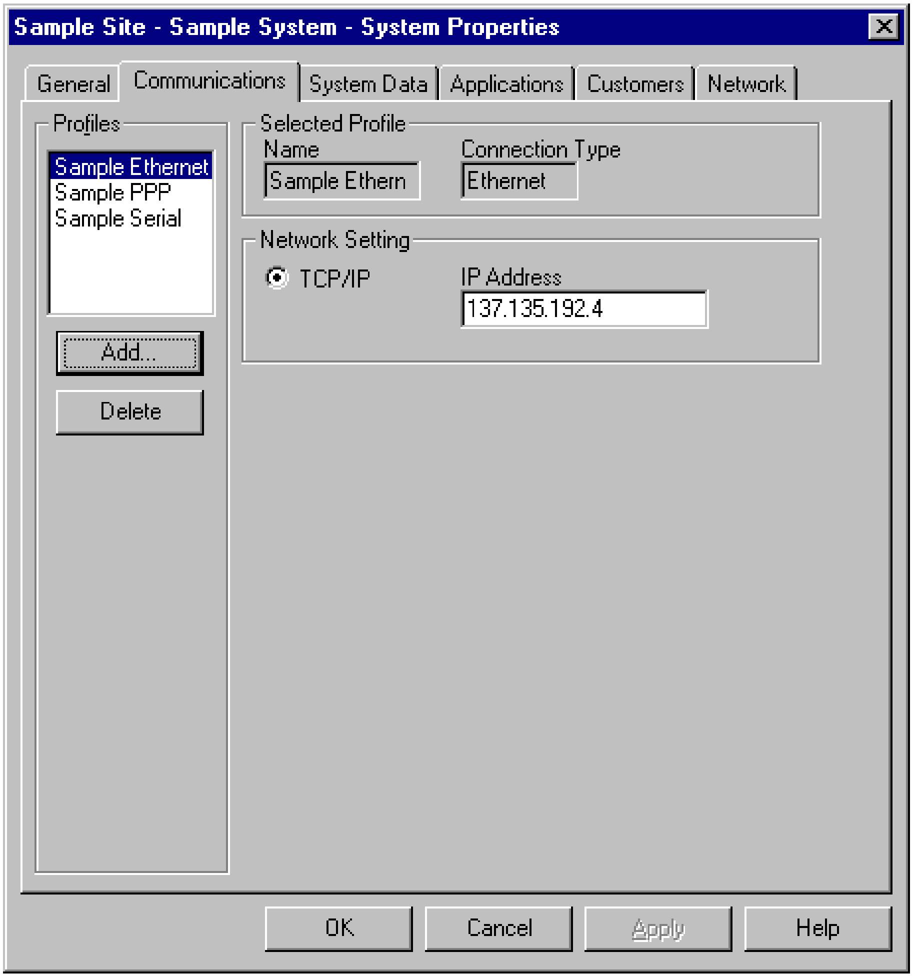
9 Enter the information in the System Properties—Communications dialog box for the connection type selected in step 6.

For an Ethernet connection type (see Figure 78 on page 144):

a. Enter the IP address that you configured on the system.

b. Click **Apply**.

Figure 78
System Properties—Communications tab—Ethernet Profile



Sample Site - Sample System - System Properties

Sample Ethernet
Sample PPP
Sample Serial

Selected Profile
Name: Sample Ethern
Connection Type: Ethernet

Network Setting
● TCP/IP
IP Address: 137.135.192.4

For a PPP connection type (see Figure 79 on page 145):

a. Enter all modem parameters and dial-up information.

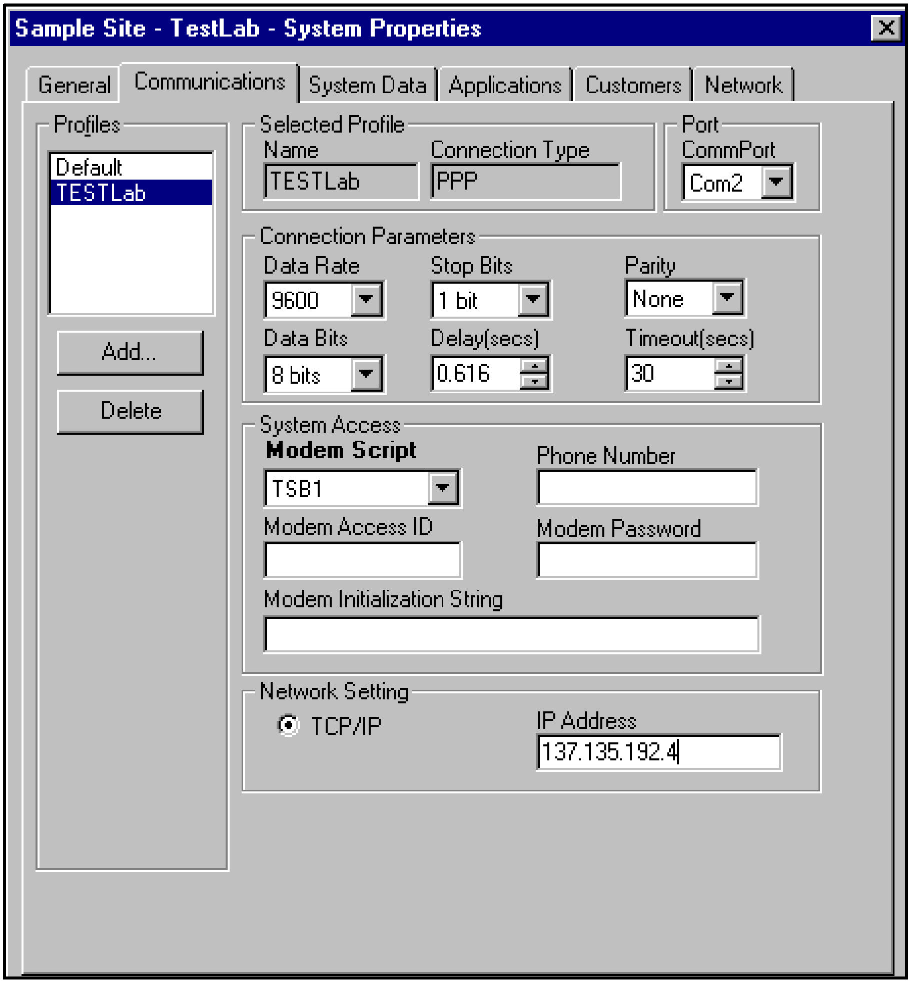
b. Select PPP in the Modem Script text box and enter the telephone number.

There may be conditions, depending on your particular installation, where you may be required to enter a modem access ID, a modem password, and a modem initialization string.

c. Set the IP address to the local IP address, as configured on the system.

d. Click **Apply**.

Figure 79
System Properties dialog box—Communications tab—PPP Profile



Profiles
Default
TESTLab

Selected Profile
Name: TESTLab
Connection Type: PPP

Port
CommPort: Com2

Connection Parameters
Data Rate: 9600
Stop Bits: 1 bit
Parity: None
Data Bits: 8 bits
Delay(secs): 0.616
Timeout(secs): 30

System Access
Modem Script: TSB1
Phone Number:
Modem Access ID:
Modem Password:
Modem Initialization String:

Network Setting
● TCP/IP
IP Address: 137.135.192.4

For a Serial connection type (see Figure 80 on page 146):

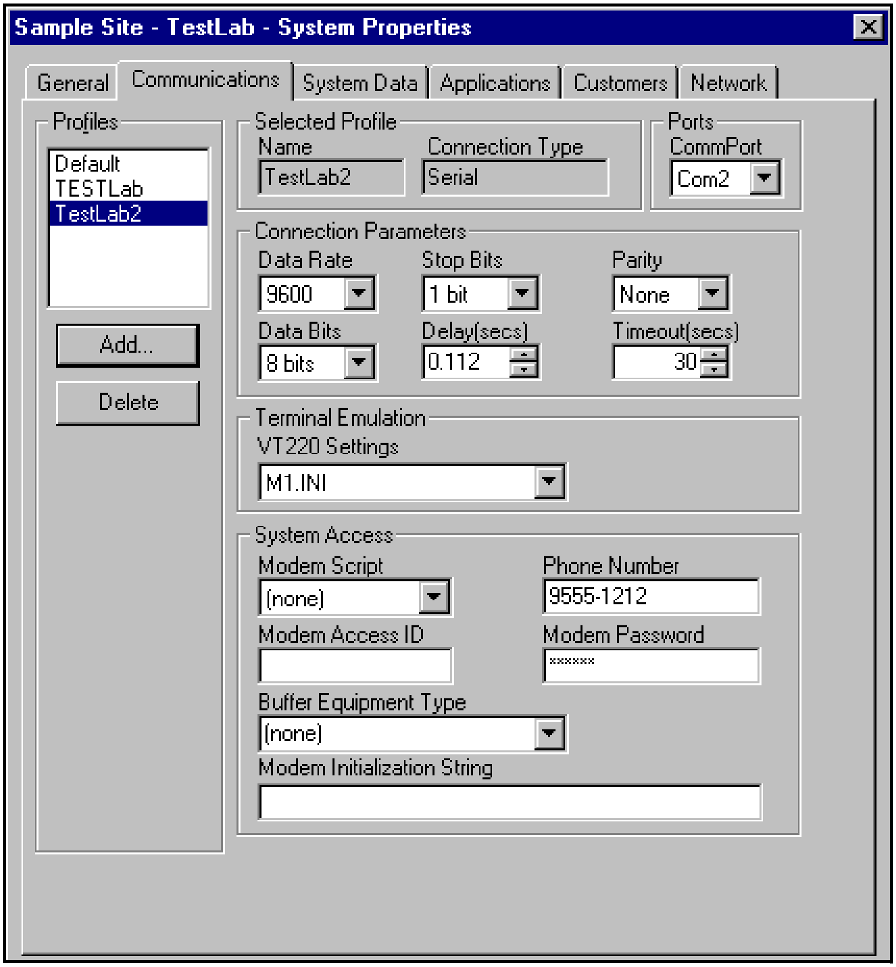
a. Enter all modem parameters and dial-up information.

b. Select the appropriate value in the Modem Script text box.

This is commonly “None” unless a specific value is defined for your system.

c. Click **Apply**.

Figure 80
System Properties dialog box—Communications tab—Serial Profile



Profiles
Default
TESTLab
TestLab2

Selected Profile
Name: TestLab2
Connection Type: Serial

Ports
CommPort: Com2

Connection Parameters
Data Rate: 9600
Stop Bits: 1 bit
Parity: None
Data Bits: 8 bits
Delay(secs): 0.112
Timeout(secs): 30

Terminal Emulation
VT220 Settings: M1.INI

System Access
Modem Script: (none)
Phone Number: 9555-1212
Modem Access ID:
Modem Password: ******
Buffer Equipment Type: (none)
Modem Initialization String:

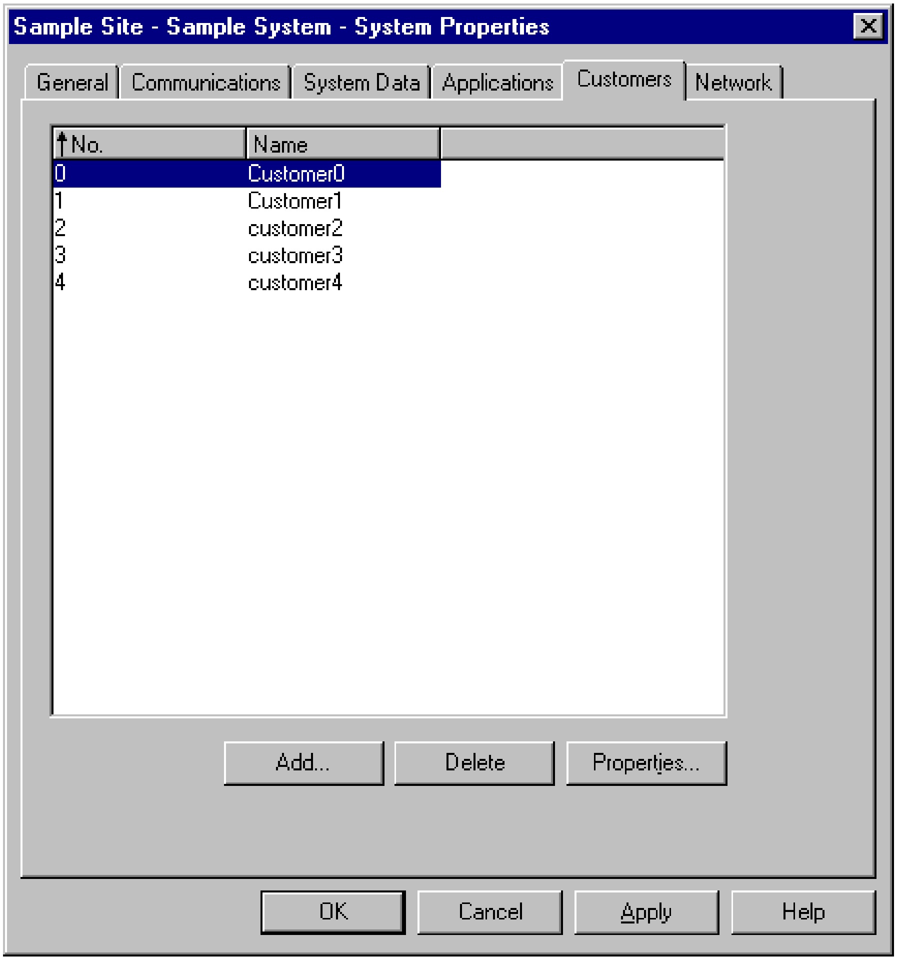
End of Procedure

Setting up customer information

Procedure 19
Setting up customer information

1 Click **Customers** tab. See Figure 81.

Figure 81
System Properties dialog box—Customers tab

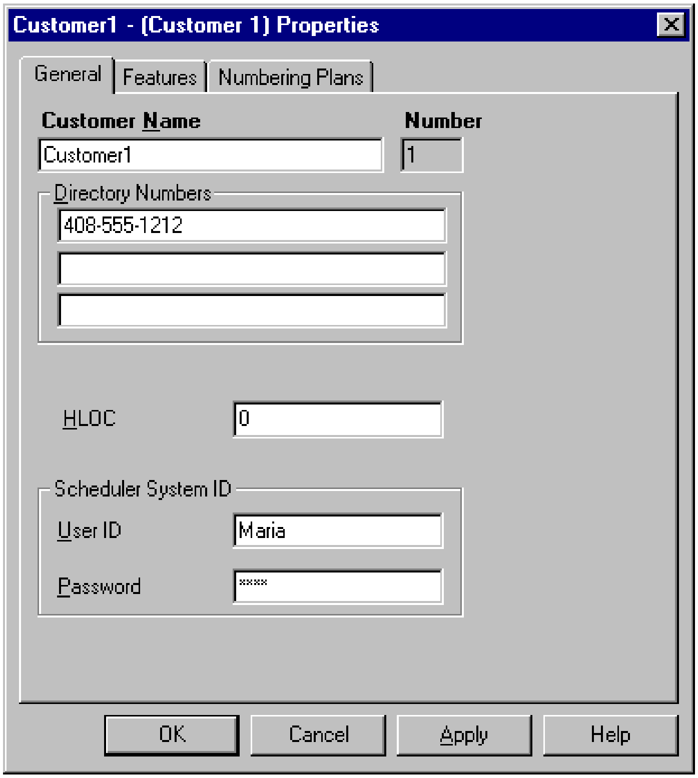


No.	Name
0	Customer0
1	Customer1
2	customer2
3	customer3
4	customer4

2 Click **Properties**.

The Customer Properties dialog box appears with the General tab selected. See Figure 82 on page 148.

Figure 82
Customer Properties—General tab



Customer1 - (Customer 1) Properties

Customer Name: Customer1

Number: 1

Directory Numbers: 408-555-1212

HLOC: 0

Scheduler System ID

User ID: Maria

Password: ****

3 In the Scheduler System ID box, change the user ID and password to one that is valid for logging onto the system, and then click **OK**.

HLOC appears the home location code (ESN) defined in LD 90.

End of Procedure

Setting up OTM applications

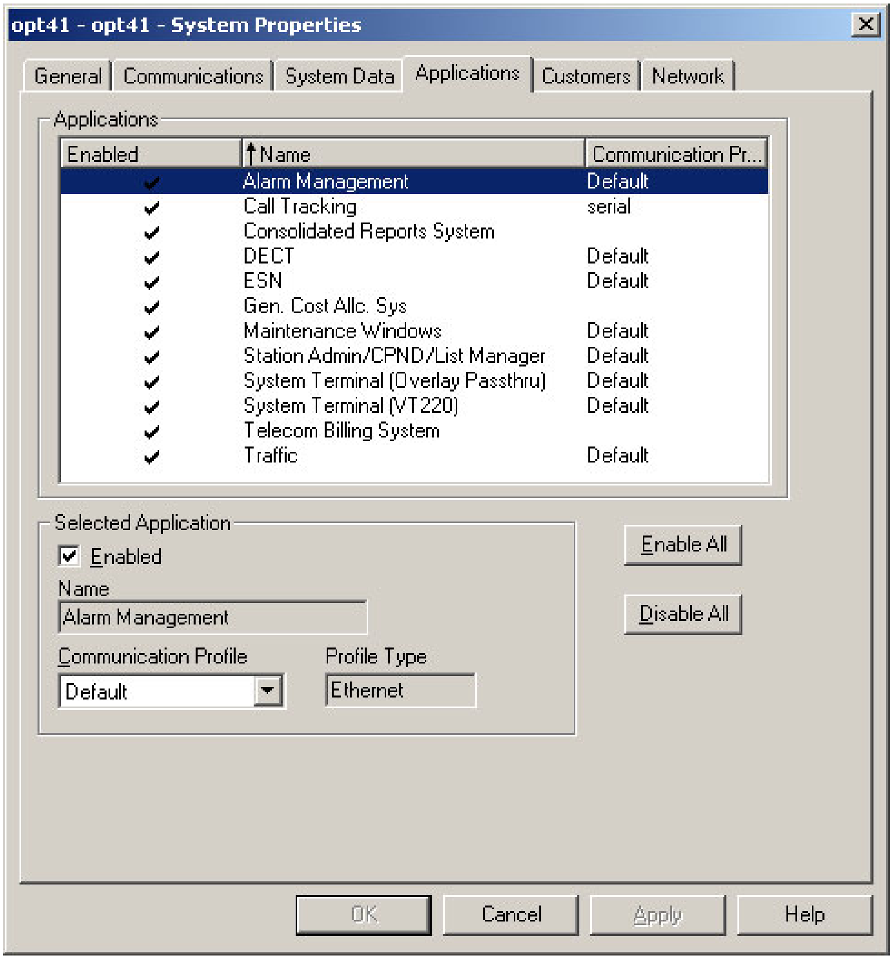
Procedure 20
Setting up OTM applications

You must enable applications to make them available in the System window.

1 Click the Applications tab.

The System Properties—Applications tab appears (Figure 83 on page 149).

Figure 83
System Properties—Applications tab



opt41 - opt41 - System Properties

Applications

Enabled	Name	Communication Pr...
✓	Alarm Management	Default
✓	Call Tracking	serial
✓	Consolidated Reports System	
✓	DECT	Default
✓	ESN	Default
✓	Gen. Cost Allc. Sys	
✓	Maintenance Windows	Default
✓	Station Admin/CPND/List Manager	Default
✓	System Terminal (Overlay Passthru)	Default
✓	System Terminal (VT220)	Default
✓	Telecom Billing System	
✓	Traffic	Default

Selected Application

☑ Enabled

Name: Alarm Management

Communication Profile: Default

Profile Type: Ethernet

2 By default, each application is selected. Modify these selections by deselecting applications.

3 Choose one the following:

a. **Enable All** : Enables the default communication profile for all available applications under the **Application** tab (with the exception of Call Tracking which is always serial).

If there is no serial profile added, then Call Tracking is not enabled. If the user has added any serial profile, then the first profile is set as the communication profile.

The General Cost Allocation System and Telecom Billing System applications are enabled without a communication profile.

b. **Disable All** : Disables the communication profile for all available applications under the **Application** tab.

4 Click **OK**.

End of Procedure

Setting up system data

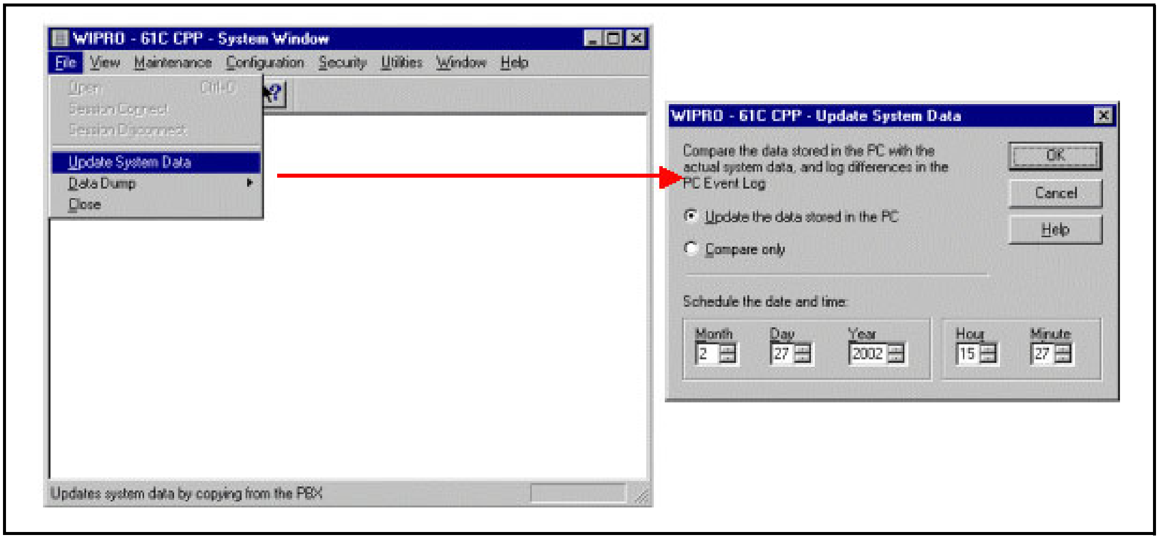
Procedure 21
Setting up system data

1 Double-click the Sample System icon to open the System window.

2 Select **File** > **Update System Data**.

3 Select **Update Data Stored in the PC**.

Figure 84
System Update



WIPRO - 61C CPP - System Window

Updates system data by copying from the PBX

WIPRO - 61C CPP - Update System Data

Compare the data stored in the PC with the actual system data, and log differences in the PC Event Log

● Update the data stored in the PC

○ Compare only

Schedule the date and time:

Month: 2
Day: 27
Year: 2002
Hour: 15
Minute: 27

4 Click **OK**.

The system data (such as the PBX type and software packages) is copied into OTM directly from the system.

Once the data is copied from the system into OTM, the test procedure is complete.

End of Procedure

Configuring a modem for OTM applications

Contents

This chapter contains information on the following topics:

Using installation tools

To ensure that a modem is configured correctly for use with Microsoft operating systems, use the modem control panel to configure it. The modem control panel automatically searches for and detects a connected modem, and then stores the configuration information in the registry for other Windows applications to access.

The same is also true for OTM applications, where the modem configuration information is obtained by searching the Windows registry with the COM port specified in the communication profile. OTM communications software then sets up the Run-Time-Container (RTC) with the modem-initialization string and communication-profile settings for the application to make its connection to the system.

Limitations

You must take into account some limitations with this process when configuring the modems:

- The Windows Modem control panel allows multiple modems to be configured on the same COM port.

  OTM software always uses the first modem found in the registry configured for the specified COM port in the communications profile. To ensure proper modem operation, configure only one modem or communication device on a given COM port.

- A factory modem-initialization (INIT) string is stored in the Windows registry. OTM applications use this INIT string to set up the modem connection.

  The OTM communications software is written to use verbal (V1) result code. If the factory INIT string is set to use numeric (V0) result code, the “Can’t set modem parameters” error message occurs and the dial-up attempt is aborted. Use the registry editor (regedit) to change the factory INIT string to use verbal (V1) result code. See the Microsoft Windows documentation for detailed instructions on how to use the registry editor, or use the following instructions.

- When searching the modem configuration information in the Windows registry, the “AttachedTo” string value is used to identify which COM port is attached to the modem.

  For a PCMCIA modem, this “AttachedTo” string value may not be available in the registry. As a result, no modem is found during the search and the RTC contains only the communication-profile settings. To correct this problem, use the registry editor (regedit) to add this “AttachedTo” string value of the COM port configured for the PCMCIA modem. See the Microsoft Windows documentation for detailed instructions on how to use the registry editor, or use the instructions below.

Configuring high-speed smart modems

As modem technology progresses, the new generation of high-speed modems provides additional functionality to achieve the highest possible connection rate. These high-speed smart modems use various tones during the handshaking period to negotiate the speed and protocol.

SDI port

The modem configured on the SDI port needs extra attention. In most cases, the modem attached to the SDI port is configured to run in dumb mode at the same speed for which the system SDI port is configured (at 9600 bps or less). This locks the modem into a specific mode of operation, preventing it from being run in command mode (echo input) or from connecting at a different baud rate than is configured for the system SDI port.

Prevent lockup

When a high-speed smart modem is used on the OTM PC to dial up the system modem, the PC modem always attempts to connect at its highest possible speed. The system’s modem, however, can only connect at the configured speed. Therefore, during the modem online handshaking period, the PC modem sends out different tones to negotiate the speed and protocol, and the switch modem connects at its configured speed and ignores additional attempts.

Once the switch modem is connected, any additional handshaking tones sent by PC modem are translated into data (garbage under this condition) and forwarded to the system SDI port. These garbage characters may eventually lock up the system port. The two modems may still be connected, but access to the system overlay input is no longer possible.

To avoid this type of problem, the key is to maintain modem compatibility. To avoid potential problems and increase the connection success rate:

- Configure the PC modem to match the switch modem's settings.
- The speed between the system SDI port and the system's modem is locked to the system SDI port's baud rate if a high-speed modem is installed on the SDI port.
- To minimize the garbage characters after carrier-detect or carrier-lost situations, set your modem S9 register to a higher value (for example, 30 = 3 seconds) and S10 register to a lower value (for example, 7 = 7/10 of a second).

  When increasing the value of the S9 register, you may need to do some timing adjustments on some of the modem/buffer equipment scripts.

Troubleshooting modem connections

The following procedures are solutions to the most common troubles.

Modem does not dial

Procedure 22
Verifying that your modem is properly configured

Verify that your modem is configured on the correct COM port:

1. From the Start menu, select **Settings > Control Panel**.
2. Open the Modems file and click **Properties**.

End of Procedure

Procedure 23
Testing the COM port

Test the COM port to which your modem is connected by launching HyperTerminal:

1. From the Start menu, select **Programs > Accessories > HyperTerminal**.

   HyperTerminal prompts you for a connection name and presents you with the telephone number dialog box.

2. In the **Connect Using** drop-down list box, select **Direct to COM *X*,** where *X* is the COM port to which your modem is connected.
3. Once you are in the terminal, type the command ***AT***.

   The modem should respond with OK.

If your modem does not respond, you may be using the wrong COM port.

End of Procedure

To verify that you are using the correct COM port:

Procedure 24
Verifying the COM port

1. In the File/Properties menu, select **Direct to COM *Y*,** where *Y* is a different COM port.
2. Once you have located the correct COM port, go back to OTM Navigator and bring up the properties for the system to which you are trying to connect.
3. Click **Communication** tab, and then choose **PPP** or **Serial** from the communication profile list.

4 Verify that the COM port you selected for this profile is the COM port on which you located your modem using HyperTerminal.

5 Verify that the baud rate matches the settings for the system port into which you dial.

End of Procedure

If the modem still does not dial:

1 Follow the steps in the procedure “Testing the COM port” on page 156 to establish a HyperTerminal connection.

2 After issuing the **`AT`** command and receiving the OK prompt, issue the command **`ATDT`*`1234567`***, where ***`1234567`*** is the telephone number for the modem connected to the system.

3 Listen to determine whether the modem dials and connects:

   a. If you do not hear the modem dialing and connecting at this point, verify that your telephone line and modem cables are connected correctly.

   b. If the modem dials and connects, verify that you have dial-up networking installed along with a dial-up-adapter.

End of Procedure

Scripting fails

In this scenario, the modem dials and connects but the Connection Details button reveals that scripting failed while waiting for a prompt.

In the Communications profile, verify that the baud rate configured for the TTY on the switch matches the baud rate configured for the modem in the PPP or Serial Communications profiles for the system to which you wish to connect. Make sure that the data bits, stop bits, and parity match as well.

Procedure 25
Viewing the Communications profiles

To view the Communications profiles for a system:

1 Right-click on the desired system in the **Navigator** window.

2 Select **Properties,** then click **Communications** tab in the Properties dialog box.

End of Procedure

Modem dials but does not connect

Procedure 26
Verifying the modem connection

1 Verify that the telephone number you are dialing is not busy.

2 Verify that you have included all necessary digits in the telephone number.

3 Check the **PPP** or **Serial Communications** profiles for the system to which you wish to connect.

To view the Communications profiles for a system:

a. Right-click on the desired system in the **Navigator** window.

b. Select **Properties**, then click **Communications** tab in the Properties dialog box.

End of Procedure

Session fails

In this scenario, the modem dials and connects and the scripting is completed successfully, but the Connection Details button reveals that the session failed.

Procedure 27
Resolving a failed session

1 Verify that the IP address that you assigned to the local PPP interface on the system is the same as the IP address you entered in the address field in the PPP Communications profile for the system to which you wish to connect.

To view the Communications profiles for a system:

a. Right-click on the desired system in the **Navigator** window.

b. Select **Properties,** then click **Communications** tab in the Properties dialog box.

2 If possible, verify that you can make an Ethernet connection to the same system:

a. After establishing a PPP connection, but before canceling the connection dialog, open a DOS command prompt: From the Start menu select **Programs > MS-DOS Prompt**.

b. Run the ping command by typing `ping 47.1.1.10` where `47.1.1.10` is the system's local IP address. See "Adding a system " in *Optivity Telephony Manager: System Administration* (553-3001-330) for information on configuring Ethernet and PPP on the system.

c. Verify that the data lights on your modem flash as the ping data is sent to the system.

If you do not receive a response from the system, verify that the IP address is the same as the one that you assigned to the local PPP interface on the system. To verify the IP address, go to the System Properties—Communication, PPP Connection Type dialog box, and confirm that the IP address that appears in the address field is correct.

End of Procedure

COM port error

In this scenario, the modem dials and connects but you receive the error message "Error writing to COM port" or "Error reading from COM port".

Procedure 28
Resolving COM port error

1 Verify that the modem you installed in Control Panel that matches your modem type.

2 Remove your installed modem driver and install a generic modem driver in its place:

   a. From the Start menu, select **Settings > Control Panel.**

   b. Double-click **Modems**.

   c. Click **Remove** to remove your modem from the installed list.

   d. Click **Add** to add a new modem driver.

   e. Select the check box **Don't detect my modem; I will select it from a list**, and then click **Next**.

   f. Select the standard modem driver matching your modem's baud rate (for example, Standard 28 800 bps Modem), and then click **Next**.

   g. Select the COM port to which your modem is connected, and then click **Next**.

   h. Click **Finish** to complete the modem installation.

   i. Restart the system, and try to establish a PPP or serial connection.

End of Procedure

Initial login

Windows users are authenticated using either a local account on the OTM server, a Windows domain account, or LDAP. There is no default login name and password for these systems.

Any user account (for example, Administrator) that is a member of the local Administrators group is always able to log in to OTM. In a new OTM installation, use any local Administrators group account for your initial log in.

After logging in to OTM for the first time, you can set up additional users and user groups by selecting the following paths:

- To add user groups, select **Security > User Groups** from the OTM Navigator window, and then select **Configuration > Add User Group...** from the User Groups window. See “Creating User Groups” in *Optivity Telephony Manager: System Administration* (553-3001-330) for detailed instructions on adding OTM user groups.
- To add users, select **Security > Users** from the OTM Navigator window, and then select **Configuration > Add User...** from the OTM Users window. See “Adding Users” in *Optivity Telephony Manager: System Administration* (553-3001-330) for detailed instructions on adding OTM users.

Users that are not created from within OTM do not appear in the OTM Users window.

Security Management

When OTM starts for the first time, the Administrator, HelpDesk, EndUser, and Default user groups are the only active user groups. You must assign access properties for any other groups that you have set up on the OTM server.

Localization

Important advice for regionalized operating systems — The name of the administrators user group in the French and German OSs is not Administrators. These names are localized by Microsoft in the regional OS software. In a default French Windows installation, the local administrators user group is “Administrateurs”. In the German version, this user group is “Administratoren”. When installed on a French or German OS, the OTM predefined administrators user group is named Administrateurs or Administratoren to match the OS.

Assigning access properties

OTM provides easy access to users for personal, system, site, or network-wide management of systems. The administrator determines the level of access for the users in a particular user group. The administrator also determines which sites and systems the members of the user group are able to manage. It is the responsibility of the network administrator to ensure that only authorized users are able to access the OTM server and its associated system.

The administrator configures Windows user groups and individual users using the Windows user interface. The administrator then determines the access permissions for each user group by using the OTM Web Navigator page. For more information about setting user access, refer to “User groups” on page 169.

Security for upgrades and re-installations

As a security precaution, with any upgrade or reinstallation of OTM software, access properties for all user groups are reset to the default values.

Administrators

Users of the OTM Administration Site belong to a distinct user group and are assigned the security profile for that user group. Users are not able to alter access permissions for the Administrators user group.

Members of the Administrators user group can:

- Log in to the OTM Administration website
- Access all OTM web applications.
- Assign access rights to the other user groups.
- Assign access rights to applications. HelpDesk users have access to all applications except those listed under Web Administration. No other user groups have any access to OTM web applications unless you specifically grant that group appropriate permissions.
- Assign access rights for web applications before any users from that group can log in.

While assigning access permissions, be certain to select the top level application for every sub-application that you assign. For example, if “System Alarms” is selected, “Equipment”must also be selected. Failure to do so can result in members of the user group being denied access to the website.

OTM web application access permissions are controlled by the Administrator on a per-user group basis. For example, the administrator may limit the OTM users access to only some of the OTM web-based functionality. The OTM Web Navigator controls access to applications by shielding web links that the user does not have access to. The directories and files comprising those applications are similarly protected.

Users

Users log in to the OTM Web Navigator using their Microsoft Windows userID and password. Login security for OTM web services ensures protection against unauthorized entry and enforces access permissions for logged-on users.

Access to web applications applies to a group, not to individual users. To change the security access for individual users, their group membership should be changed. For information about setting user access, refer to “User groups” on page 169.

With the exception of Administrators, do not place a person in multiple groups. The first group detected by OTM is used to determine access permissions. There is no restriction on the Administrators group. Users may belong to other groups, but if they belong to the Administrators group, the Administrators profile overrides all other profiles.

There is a Default user category. Default users are able to successfully log in to the Web Navigator, but they do not have a user group defined in their Directory record.

OTM administrators and Help desk users have user accounts in a Windows domain. End users may have accounts either in a Windows domain or through an LDAP server.

OTM administrators and Help desk users can access and change their own telephones through either the Web Navigator or the Desktop Services end user pages. Access to the end-user pages requires the appropriate OTM directory setup (user login and user group) for these administrators and Help desk users.

Authentication

Authentication requests are passed to OTM Watchdog, which applies the configured authentication method and creates a session for the user. For authentication on “Local OTM server account” or “Windows Domain account,” the standard Windows Security Provider is used. For authentication using LDAP, the login name and the password are passed to the LDAP server.

In OTM, Windows and web users are authenticated using the settings configured either on the User Authentication web page or in the User Authentication dialog box. The information that appears on the web page and in the dialog box is identical. The web link to the User Authentication page is found under web administration in the OTM Web Navigator tree. The User Authentication dialog box is accessed from the Security menu in the OTM Windows Navigator.

Authentication methods

The following user authentication methods are available:

- Local OTM server account
- Windows Domain account
- LDAP authentication

You can select any one of the three methods or a combination of the these methods to authenticate users on all OTM platforms: OTM server, OTM Windows client, and OTM web client.

The Administrator account is always authenticated as a Windows local account. This is due to the fact that the Administrator account is the default account on these Windows platforms.

The default authentication method is “Local OTM server account.” Since this method does not require a search of the OTM Directory to find the user’s assigned user group, the “Local OTM server account” method provides the best login performance.

If you choose multiple authentication methods, OTM respects the order configured; however, it should be noted that the best performance is achieved by using the “Local OTM server account” method.

For information on configuring authentication methods using the User Authentication web page, see “User authentication” in *Optivity Telephony Manager: System Administration* (553-3001-330).

For information on configuring authentication methods using the User Authentication Windows dialog box, see “User authentication” in *Optivity Telephony Manager: System Administration* (553-3001-330).

Password policy

Password security during transport across the network is accomplished in the following manner:

Default passwords on the Call Server, Signalling Server and the Voice Gateway Media Card are forced changed by the software.

OTM uses the PWD1, PWD2 and PDT passwords for certain functions that interact with the Call Server, Signalling Server and Voice Gateway Media Card.

If any of the passwords expire due to the force change feature, OTM functionality fails similar to having incorrect passwords.

The passwords must be updated manually on the Call Server, Signalling Server and Voice Gateway Media Card through CLI commands. OTM system properties must also be updated with the new passwords before proceeding with any OTM functionality.

- OTM Windows client passwords are encrypted using Crypto APIs prior to being transmitted. The same private key is used by both the client and the server.

- For OTM web clients, by default, clear text passwords are used; however, if the OTM server has the proper certificate installed, you can force the use of SSL encrypted transport during authentication. To use the SSL during the authentication process, the OTM server must have the required certificate installed as described in "Configuring Secure Sockets Layer (SSL)" on page 131. Click the **Use SSL for web login authentication** check box after installing the certificate..

  Before using SSL on the OTM server, the OTM server must have the required certificate installed as described in "Configuring Secure Sockets Layer (SSL)" on page 131. If "Use SSL for web login authentication" is selected, web login is performed using https://... instead of http://... and traffic is encrypted. The OTM server automatically switches to non-SSL transport once the user is successfully authenticated.

- If LDAP authentication is used, the following sequence is used:
  - The OTM server tests to determine whether the Directory server offers SSL-based authentication.
  - If SSL is supported by the Directory server, passwords are encrypted before being transmitted using a Public-Private key pair negotiated through the LDAP mechanism.
  - If SSL is not supported, passwords are transmitted as clear text.
- All passwords, including passwords to access the system, are stored in the OTM database in an encrypted format. Crypto API, the standard Windows Security Provider encryption service, is used for this purpose.

Blank passwords

OTM does not support blank passwords.

User management

There are two major categories of users within OTM — Navigator users and end users. You control access for these users by configuring Navigator users in the OTM Users window, and end users in the Employee Editor.

Navigator users

OTM Windows Navigator and Web Navigator users are managed through OTM User administration. Users are created and assigned to a particular user group. This user group assignment controls access to OTM Windows and web applications.

There are two different types of Navigator users:

- Local — Local Navigator users have accounts that exist on the OTM server. When a user is added, an OTM user account and a corresponding local Windows user account are created on the OTM server. The new user is assigned to the selected Windows user group.

  Delete an OTM user account to remove the user account from the account list, as well as from all relevant database tables.

- Remote — Remote Navigator users have accounts that reside on a domain controller or in an LDAP Directory. You use OTM User administration to assign the Remote Navigator user's login name to an OTM user group.

For information on configuring Navigator users, see "Configuring OTM Navigator users" on page 171.

End users

End users access the OTM Desktop Services website to view information on, and make changes to, their telephones.

Although end users can be given an OTM user account similar to Navigator users, they typically are authenticated through a Windows domain account or an LDAP-compliant directory.

For end users, the following attributes are entered into the users record in the OTM Directory via the Employee Editor:

- Login name — The login name is used to associate the end users with their telephones.
- User group — The user group assignment determines what the end users can view and change on their telephones.
- Reporting Access Rights — Reporting Access Rights controls access to the web TBS telecom billing reports.

For information on using the Employee Editor to configure end users for access to OTM, see the *Optivity Telephony Manager: System Administration* (553-3001-330).

Login process

This chapter describes the activities performed by OTM to authenticate and log in OTM users.

Procedure 29
Login process

1 The user accesses the Windows login dialog box or the web login page.

2 User enter their login name and password.

3 OTM performs authentication respecting the configured order.

4 If authentication is successful, user group resolution is performed as follows:

Navigator login — Windows or web

— If the user is authenticated using a local OTM server account, user group resolution is performed using the local account database.

— If the user is authenticated using a Windows domain account, user group resolution is performed using the OTM user database. If the user group mapping is not found in the OTM user database, the OTM directory is used.

— If the user is authenticated using an LDAP Directory, user group resolution is performed using the OTM user database. If the user group mapping is not found in the OTM user database, the OTM directory is used.

If the user cannot be mapped to a user group, OTM appears the following message: “You have not been assigned to an OTM user group. Please contact the OTM Administrator.”

— End users — web only: User group resolution is performed using the OTM directory. If users are not found, they are assigned to the default user group.

End of Procedure

User groups

OTM user groups provide the mechanism to control access to the following OTM resources:

- OTM Windows Navigator — Navigator and site/system level applications
- OTM Web Navigator — Navigator and site/system level applications
- Access to web Station Administration — web Desktop Services for end users

In addition, OTM provides the following user management functions:

- The ability to create/delete users and user groups (Windows user interface only)
- The ability to configure web Desktop Services for end users (web user interface only)

Creating a user group

The Windows user group application was known as User Templates in early versions of OTM. New user groups are created using an existing user group as the base.

User groups provided with OTM

The following user groups and access definitions are shipped with OTM:

- Administrators — This user group has read/write access to all sites, systems, and applications. The Administrators user group cannot be changed, renamed, or deleted.

  The other user groups provided with OTM can be changed, but they cannot be renamed or deleted.

- HelpDesk — This user group has the following access privileges:
  - Access to all Web Navigator tree items except those located under the web Administration branch
  - Full access to web Desktop Services, including read/write and synchronization capabilities
  - Full access to the Windows Navigator applications with the exception of IP line/ IP Trunk Services
- EndUser — This user group has the following access privileges:
  - No access to the OTM Windows or web applications
  - web Desktop Services is read-only; however, all except 21 of the most commonly used features are set to “Hidden”
- Default — This user group has no access to any OTM features or applications.

User management recommendations

The Administrator user account for the Windows OS does not appear in the OTM Users window. This is to prevent users from changing the Administrator account password from within OTM.

Even though it is not listed in the Users window, you can always use the OS Administrator account to log in to OTM.

Nortel strongly recommends that a new user group be created in OTM based on the Administrators user group. OTM users should be assigned to this new user group instead of adding them to the Administrators user group. This is a security measure to ensure that a user with administrative access to OTM does not also have access to the OS on the OTM server as a member of the Administrators group.

Installation

Fresh installation

In a fresh installation, three new user groups are created in Windows. OTM utilizes HelpDesk, EndUser, and Default user groups along with the existing Administrators group.

For OTM Windows clients, the OTM server's host name must be provided during installation. The host name is saved in the registry.

Upgrade

In an upgrade, existing OTM Windows Templates are created as user groups. By default, these groups do not have access to OTM Web Navigator applications.

A local server account is created for each existing OTM Windows user. The new account is assigned to the appropriate user group.

Existing OTM Telephone Access Profiles, which were based on user groups, are migrated from the Web Navigator database to the new user group database. This assumes that the corresponding groups related to them already exist.

These user groups are also migrated to the web Station database; however, new user groups do not have access to web Station administration. You must configure access to web Station Administration using the User Groups web page. See "User groups" on page 189.

Configuring OTM Navigator users

OTM allows you to create user groups to speed the process of adding users accessing the OTM Windows Navigator and certain OTM web-based applications. In the User Group Properties dialog box, you define most aspects of a certain kind of user, such as level of access to sites and systems, and automatic connection to particular systems. You can create as many user groups as you need. You assign individual users to a user group when you add users to the OTM database.

There are two types of users — local users and remote users. Local users have accounts on the OTM server. When you add a new local user, an OTM user account and a local Windows user account are created and the account is assigned to the specified user group. Deletion of a user removes the user account from the account list in Windows, as well as from all relevant database tables. Remote users have accounts that exist on a domain controller or in an LDAP-compliant directory. For these users, OTM is used to assign the login name for the account to an OTM user group. The login names defined in OTM must be unique for all users.

Access to OTM Windows and web applications is provided through the Windows server. A Windows domain account or an LDAP-compliant directory can also be used to authenticate OTM users for web Services. Refer to "Web Navigator" in *Optivity Telephony Manager: System Administration* (553-3001-330).

Deleting a user group

You can delete a user group only after all associated members of that group are either deleted or reassigned to another user group.

You cannot delete the account that you used when you logged in to your current session.

Restricting user access permission levels

You can restrict a user from having access to sites, systems, and applications. However, when a user is defined as being restricted from any access to all sites, systems, and applications in the Navigator, the user can, in fact, see all the sites and systems in the Navigator tree and has read-only access to their properties. If restricted users try to open a system, they see a System Window with no applications visible.

Sites and systems displayed in user groups

When adding or modifying a user group, only systems that have applications enabled are presented. If no applications are enabled for the systems within a given site, the site and system(s) do not appear in the User Group Properties dialog box.

For information on configuring end users for access to the OTM website, see "User groups" on page 189.

User authentication

You can select any of the following three methods or combination of these methods to authenticate OTM users:

- Local OTM server account
- Windows NT Domain account
- LDAP authentication

The Administrator account is always authenticated through the local server account because it is a default account on all supported Windows platforms.

The default authentication method is the Local OTM server account. This method provides the best login performance because there is no requirement to search the OTM directory for the user's assigned user group.

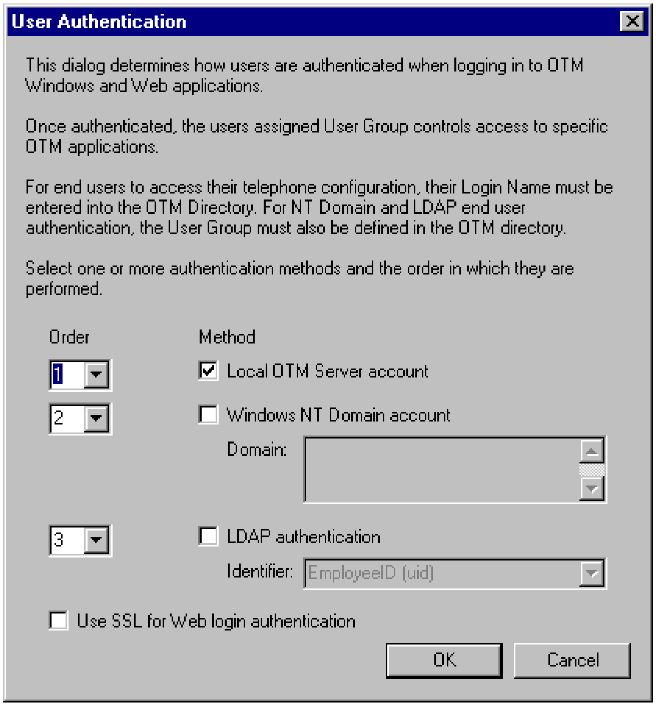
You can also configure user authentication using the OTM web Services. For information, see "User authentication" on page 187.

Procedure 30
Configure authentication

1 From the OTM Windows Navigator, select **Security > User Authentication**.

The User Authentication dialog box opens (Figure 85).

Figure 85
User Authentication dialog box



User Authentication

This dialog determines how users are authenticated when logging in to OTM Windows and Web applications.

Once authenticated, the users assigned User Group controls access to specific OTM applications.

For end users to access their telephone configuration, their Login Name must be entered into the OTM Directory. For NT Domain and LDAP end user authentication, the User Group must also be defined in the OTM directory.

Select one or more authentication methods and the order in which they are performed.

Order	Method
1	☑ Local OTM Server account
2	☐ Windows NT Domain account Domain:
3	☐ LDAP authentication Identifier: EmployeeID (uid)

☐ Use SSL for Web login authentication

2 Use the check boxes to select one or more of the available authentication methods.

a. If you select Windows NT Domain account, enter one or more domains in the Domain text box. Separate the domain names with a comma.

Note: You must separate the domain names with a comma. Do not use any spaces.

b. If you select LDAP authentication, use the drop-down list to choose either EmployeeID (uid), or Email (email).

3 Use the drop-down lists to assign the order in which the authentication methods are performed.

If you choose multiple authentication methods, OTM respects the order configured; however, it should be noted that the best performance is achieved by using the "Local OTM server account" method.

4 To use the SSL during the authentication process, the OTM server must have the required certificate installed as described in "Configuring Secure Sockets Layer (SSL)" on page 131. Select the **Use SSL for web login authentication** check box after installing the certificate.

If the OTM server has the required certificate installed, selecting the check box causes OTM to use SSL-encrypted transport during authentication. In this case, web login is performed using https:// rather than http://, and the traffic is encrypted. The OTM server automatically switches to non-SSL transport once the user is successfully authenticated.

The selected method(s) are used to authenticate users on all OTM platforms: OTM server, OTM client, and OTM web client.

End of Procedure

Creating a user group

OTM allows you to create User Groups to speed the process of adding users by accessing the OTM Windows Navigator and certain OTM web-based applications. In the User Group Properties dialog box, you define most aspects of certain kinds of users, such as their level of access to sites and systems and automatic connection to particular systems. You can create as many User Groups as you need. You assign individual users to a User Group when you add users to the OTM database.

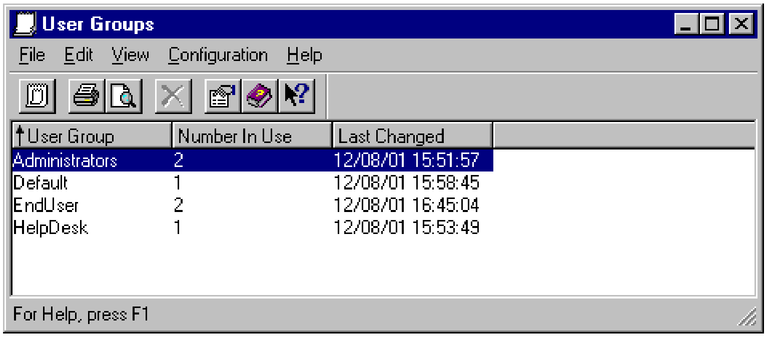
There are two types of users: local users and remote users. Local users have accounts on the OTM server. When you add a new local user, an OTM user account and a local user account are created, and the account is assigned to the specified User Group. Deletion of a user removes the user account from the account list as well as from all relevant database tables. Remote users have accounts that exist on a domain controller or in an LDAP-compliant directory. For these users, OTM is used to assign the user ID for the account to an OTM user group. The login names defined in OTM must be unique for all users.

Access to OTM web Services is provided through the server. Refer to "User authentication" on page 187.

Procedure 31
Creating a user group

1 In the Navigator window, choose **Security > User Groups** to display the User Groups window (Figure 86).

Figure 86
User Groups window

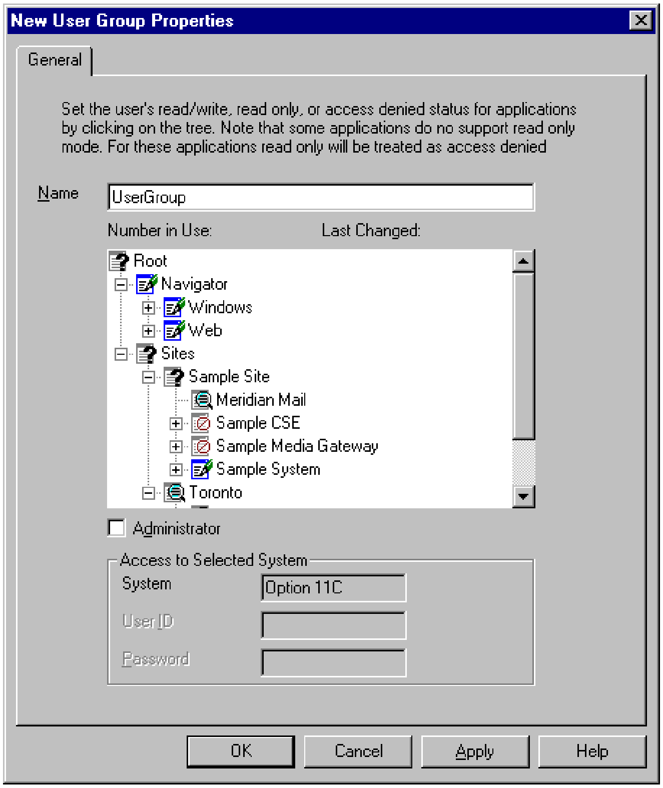


User Group	Number In Use	Last Changed
Administrators	2	12/08/01 15:51:57
Default	1	12/08/01 15:58:45
EndUser	2	12/08/01 16:45:04
HelpDesk	1	12/08/01 15:53:49

2 Choose **Configuration > Add User Group**. The new user group is created with the same access privileges as the highlighted user group. The New User Group Properties dialog box opens (Figure 87).

The Administrators, Default, EndUser, and HelpDesk User Groups are always available and cannot be deleted. You can modify all groups except for Administrators. The Administrators User Group has access to all Windows-based and web-based OTM applications.

Figure 87
New User Group Properties dialog box



New User Group Properties

Set the user's read/write, read only, or access denied status for applications by clicking on the tree. Note that some applications do no support read only mode. For these applications read only will be treated as access denied

Name UserGroup

Number in Use:

Last Changed:

□ Administrator

Access to Selected System

System Option 11C

User ID

Password

3 Enter a name for this User Group.

For each site, system, and application in the tree, use the right mouse button to assign user privileges (**Read-write**, **Read-only**, **or No Access**). Each click of the right mouse button causes the access privileges and corresponding icon to change. Select the Administrator box, if appropriate. The site and system icons change to reflect the access level.

Access privileges defined for sites or systems at higher levels in the tree structure are applied to all subordinate items. See Table 11 on page 177.

The question mark icon indicates that the sub-items belonging to the item displaying the question mark icon have mixed access settings.

Table 11
Access privilege icons

Icon	Explanation
✎	Read and write access
🔍	Read only access
⊘	No access
?	Indicates that the access privileges in the branch are mixed between one or more of the above levels

4 Enter values in the User ID and Password text boxes to allow this class of user to connect to this system without having to enter a User ID and Password each time you want to connect.

If the Administrator wants to use the web Maintenance Pages, these fields must be completed in the Administrators User Group properties.

5 Click **OK** to save changes and close the User Group Properties dialog box.

End of Procedure

Adding a user

The “Administrator” user account for the Windows 2000 OS does not appear in the OTM Users window. This is to prevent users from changing the Administrator account password from within OTM.

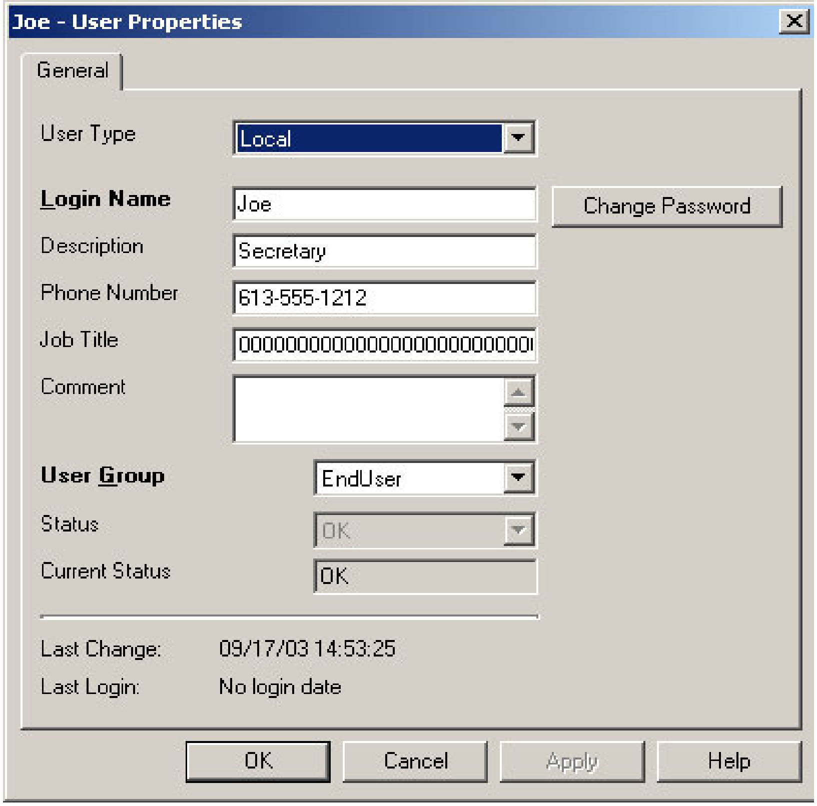
Even though it is not listed in the Users window, the OS Administrator account can always be used to log in to OTM.

Procedure 32
Adding a user

1 In the OTM Users window, choose **Configuration** > **Add User**.

The New User Properties dialog box opens. See Figure 88.

Figure 88
New User Properties dialog box



Joe - User Properties

General

User Type: Local

Login Name: Joe

Description: Secretary

Phone Number: 613-555-1212

Job Title: 000000000000000000000000000

Comment:

User Group: EndUser

Status: OK

Current Status: OK

Last Change: 09/17/03 14:53:25

Last Login: No login date

2 Select a User Type from the drop-down list:

   - Local - Users who are authenticated using an account on the OTM server.
   - Remote - Users who are authenticated using LDAP or domain.

   When Remote is selected, the Change Password button, as well as the Status and Current Status controls, are disabled.

3 Enter a User ID.

4 From the User Group drop-down list, select the group to use as the basis for this user definition.

5 Enter other data as required.

6 Click **Apply**. OTM prompts you to enter a password.

7 Enter the password and click **OK** to change the OTM login password for this user only.

8 Click **OK**. The new user appears in the OTM User window. Close the OTM User window.

End of Procedure

Authenticating users

You can select one of the following methods to authenticate OTM users:

- Local OTM server account
- LDAP authentication

The Administrator account is always authenticated through the local server account because it is a default account on all supported Windows platforms.

The default authentication method is the Local OTM server account. This method provides the best login performance because there is no requirement to search the OTM directory for the user’s assigned User Group.

Procedure 33
Authenticating users

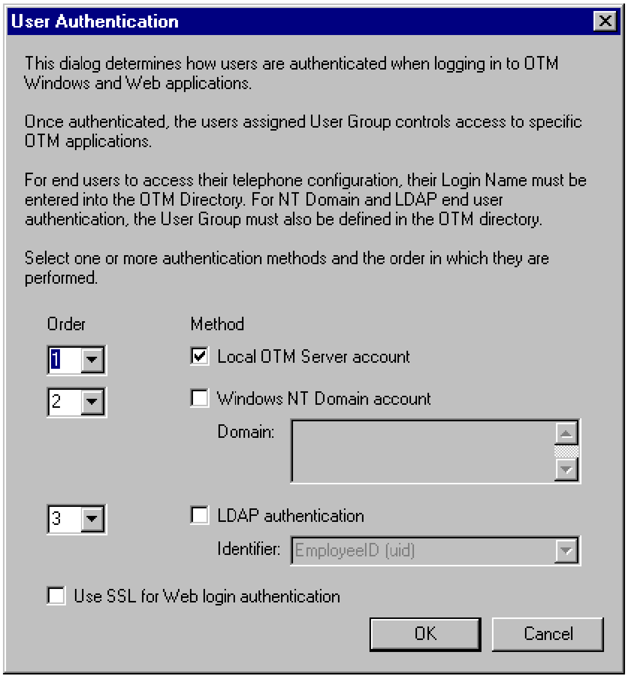
To configure authentication:

1 From the OTM Windows Navigator, select **Security > User Authentication**.

   The **User Authentication** dialog box appears. See Figure 89 on page 180.

   Authentication methods can also be configured using the web navigator. See “User authentication” on page 187.

Figure 89
User Authentication dialog box



User Authentication

This dialog determines how users are authenticated when logging in to OTM Windows and Web applications.

Once authenticated, the users assigned User Group controls access to specific OTM applications.

For end users to access their telephone configuration, their Login Name must be entered into the OTM Directory. For NT Domain and LDAP end user authentication, the User Group must also be defined in the OTM directory.

Select one or more authentication methods and the order in which they are performed.

Order	Method
1	☑ Local OTM Server account
2	□ Windows NT Domain account Domain:
3	□ LDAP authentication Identifier: EmployeeID (uid)

□ Use SSL for Web login authentication

2 Use the check boxes to select one or more of the available authentication methods. If you select LDAP authentication, use the drop-down list to choose either **EmployeeID (uid)**, or **EMail** (email).

3 Use the drop-down lists to assign the order in which the authentication methods are performed.

If you choose multiple authentication methods, OTM respects the configured order; however, it should be noted that the best performance is achieved by using the Local OTM server account method.

4 To use SSL during the authentication process, the OTM server must have the required certificate installed as described in "Configuring Secure Sockets Layer (SSL)" on page 131. Click the **Use SSL for web login authentication** check box after installing the certificate.

If the OTM server has the required certificate installed, setting the check box causes OTM to use SS- encrypted transport during authentication. In this case, web login is performed using https:// rather than http://, and the traffic is encrypted. The OTM server automatically switches to non-SSL transport once the user is successfully authenticated.

5 The selected method(s) are used to authenticate users on all OTM platforms: OTM server, OTM client, and OTM web client.

End of Procedure

Adding OTM web users

Contents

This chapter contains information on the following topics:

Overview

This chapter contains information on:

- Web capabilities
- User login and security
- Access permissions
- User authentication
- User groups
- Desktop services

Access to the OTM web is set up using the users and groups functionality in Windows® 2000. User authentication can also be accomplished using LDAP. Domain accounts and LDAP authentication are normally used for end users who access web Desktop Services to administer their telephones.

Capabilities

The OTM web provides the following:

- A list of systems and devices; users click on a system or device to:
  - — open a web System Terminal or URL to manage a system or device
  - — open Maintenance Pages for performing maintenance operations on system hardware
- web-based alarm browser to view alarms and events from multiple systems and devices
- ability to locate telephones, view, and change configuration data
- web-based Maintenance Pages to perform maintenance operations (enable, disable, and so on) on system hardware
- OTM web configuration pages (login access, LDAP sync reports, and so on)

The OTM administrator has the responsibility of installing, configuring, and maintaining OTM web services.

User login and security

Users log in to the OTM web using their Windows userID and password. Login security for OTM web services ensures protection against unauthorized entry and enforces access permissions for logged-on users.

There are three categories of users:

- Administrators — OTM administrators
- HelpDesk — OTM Help desk users
- EndUser — OTM end users

In addition, there is a Default user category. Default users are able to successfully log in to the Web, but they do not have an access profile defined in their Directory record.

OTM administrators and Help desk users have user accounts in a Windows domain. End-users may have accounts either in a Windows domain or through an LDAP server. Administrators must be set up in a Windows Administrator group on the server itself, not on a remote computer.

OTM administrators and Help desk users can access and change their own telephones through either the Web or the Desktop Services end user pages. Access to the end-user pages requires the appropriate OTM directory setup (user login and user group) for these administrators and Help desk users.

OTM web application access permissions are controlled by the administrator on a per-Windows user group basis. For example, the administrator may limit the OTM user's access to only some of the OTM web-based functionality. The OTM web controls access to applications by shielding web links to which the user does not have access. The directories and files comprising those applications are similarly protected.

Configure Windows® 2000 user groups and individual users using the Windows user interface on the OTM server then determine the access permissions for each user group by using the OTM web page. For information about setting user access, refer to "User groups" on page 189.

Precaution

As a security precaution, with any upgrade or reinstallation of OTM software, access profiles for all user groups except Administrator are reset. By using the web Access Security feature, any member of the Administrator user group can log in and set up access profiles for members of the HelpDesk, end-user, and default plug-ins.

Plug-ins

When an administrator or HelpDesk user first points a browser to the OTM Navigator website, a check is performed to see if the user has the required OTM Java plug-in. If the plug-in is not installed, the administrator or Help desk user is given the option of downloading and installing the plug-in. This operation is similar to the standard download operations in that the user must download the plug-in to the user's hard disk, and then it installs itself onto the computer.

While the plug-in check is being performed, the OTM splash screen appears. If the plug-in is installed, or after installation of the plug-in, the user is taken to the login page.

Default URL

The default OTM URL is the end user login page. To navigate to the administrator login page, place **/admin** after the OTM IP address or host name.

Access permissions

When OTM starts for the first time, the Administrator profile is the only active profile. You must assign access permissions for the other Windows XP or Windows 2000 Groups that you have set up on the OTM server.

Administrator Group access permissions

Persons belonging to the Administrators user group on the OTM server can log in to the OTM website and get unrestricted access. The Administrators group has unrestricted access by default. You are not able to alter access permissions for the Administrators user group.

Users of the OTM Administration Site belong to a distinct user group and are assigned the security profile for that user group. For example, the Administrators user group has access to all web applications.

French or German OS Administrator groups

Important advice for localized OS — The name of the administrators user group in the French and German operating systems is not Administrators. These names are localized by Microsoft in the regional operating system software. In a default French installation the local administrators user group is “Administrateurs”. In the German version, this user group is "Administratoren". When installed on a French or German OS, the OTM predefined administrators user group is named Administrateurs or Administratoren to match the OS.

User group access rights

You, the network administrator, log in to the OTM Administration website and assign access rights to the other user groups. By default, a member of any group other than Administrators does not have any access to OTM web applications unless you specifically grant that group appropriate permissions.

From the User Groups page, you grant or deny access to web applications to a group, not to individual users. To change the security access for individual users, their group membership should be changed. For new groups, the Administrator must assign access rights for web applications before any users from that group can log in. For information about setting user access, refer to “User groups” on page 189.

With the exception of Administrators, do not place a person in multiple groups. The first group detected by OTM is used to determine access permissions. There is no restriction on the Administrators group. Users may belong to other groups, but if they belong to the Administrators group, the Administrators profile overrides all other profiles.

While assigning access permissions, be certain that you select the top-level application for every sub-application that you assign. For example, if you are selecting System Alarms, you must also select Equipment. Failure to do so can result in members of the user group being denied access to the website.

User authentication

You can select one of the following methods to authenticate OTM users:

- Local OTM server account
- Windows domain account
- LDAP authentication

The Administrator account is always authenticated through the local server account because it is a default account on all supported Windows platforms.

The default authentication method is the Local OTM server account. This method provides the best login performance because there is no requirement to search the OTM directory for the user's assigned User Group.

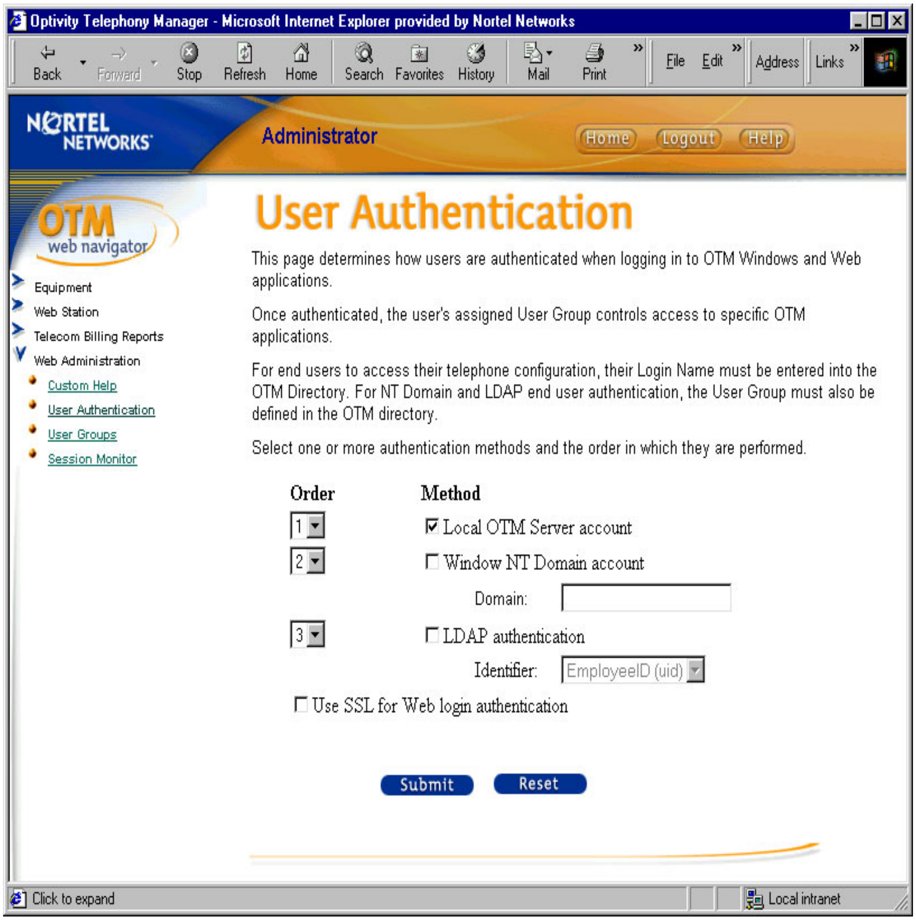
Procedure 34
Configuring authentication

To configure authentication:

1 Under Web Administration in the OTM web tree, select **User Authentication.**

The User Authentication page appears. See Figure 90 on page 188.

Figure 90
User Authentication page



User Authentication

This page determines how users are authenticated when logging in to OTM Windows and Web applications.

Once authenticated, the user's assigned User Group controls access to specific OTM applications.

For end users to access their telephone configuration, their Login Name must be entered into the OTM Directory. For NT Domain and LDAP end user authentication, the User Group must also be defined in the OTM directory.

Select one or more authentication methods and the order in which they are performed.

Order	Method
1	☑ Local OTM Server account
2	☐ Window NT Domain account
	Domain:
3	☐ LDAP authentication
	Identifier: EmployeeID (uid)

☐ Use SSL for Web login authentication

2 Use the check boxes to select one or more of the available authentication methods. If you select LDAP authentication, use the drop-down list to choose either EmployeeID (uid), or EMail (email).

3 Use the drop-down lists to assign the order in which the authentication methods are performed.

If you choose multiple authentication methods, OTM respects the configured order; however, it should be noted that the best performance is achieved by using the Local OTM server account method.

4 To use the SSL during the authentication process, the OTM server must have the required certificate installed as described in "Configuring Secure Sockets Layer (SSL)" on page 131. Click the **Use SSL for web login authentication** check box after installing the certificate.

If the OTM server has the required certificate installed, selecting the check box causes OTM to use SSL-encrypted transport during authentication. In this case, web login is performed using https:// rather than http://, and the traffic is encrypted. The OTM server automatically switches to non-SSL transport once the user is successfully authenticated.

5 The selected method(s) are used to authenticate users on all OTM platforms: OTM server, OTM client, and OTM web client.

End of Procedure

For information on configuring users for desktop access, see "Enable web desktop access in the OTM Directory" on page 199.

Authentication methods can also be configured using the Windows navigator. See "User authentication" on page 187.

User groups

Navigator access is controlled by user group. A user's user group assignment determines which features are available on the Telephone features page. You also use the User Groups page to indicate which users are permitted to make changes to the General and Keys pages.

User groups must be added and deleted in the OTM Windows Navigator.

OTM is shipped with the following user groups and corresponding access rights:

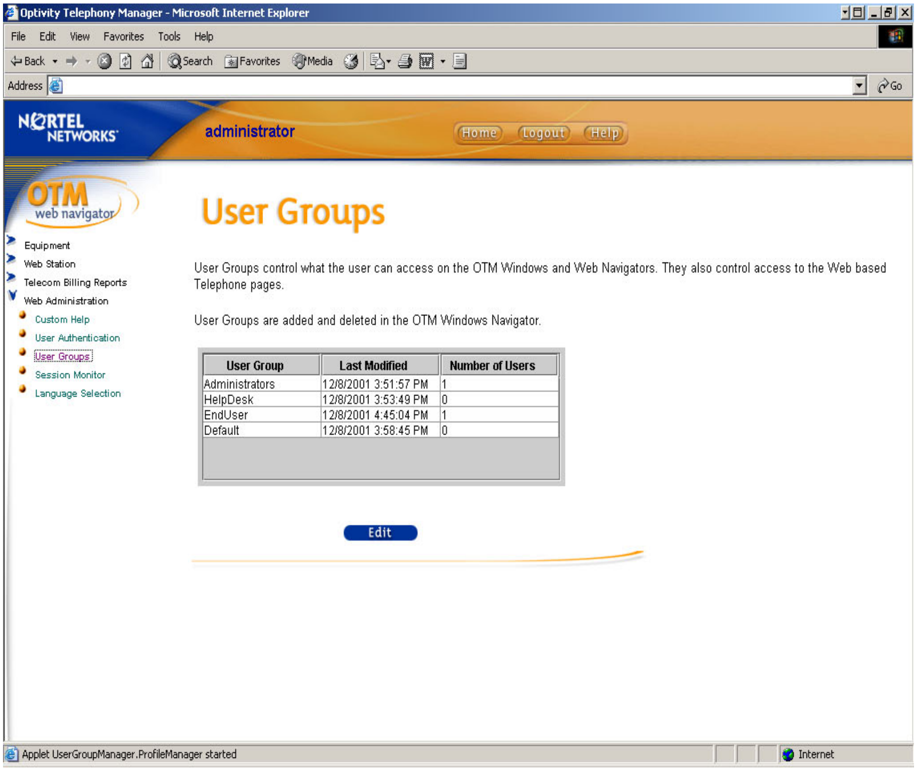
- Administrators
  - — Full read/write access rights. Access rights cannot be changed for this user group.
- HelpDesk
  - — Full access to all Web tree items except those under Web Administration.
  - — Full access to web Desktop Services, including read/write and synchronization capabilities.
  - — Full access to Windows Navigator applications with the exception of ITG Services.

- EndUser
  - — No access to Web or Windows Navigator applications.
  - — Web Desktop Services is read-only. Only 21 features are available; the rest are hidden.
- Default
  - — No access.

To view the available user groups, click the **User Groups** link located under Web Administration in the OTM web tree.

The **User Groups** page appears. See Figure 91.

Figure 91
User Groups page



User Groups

User Groups control what the user can access on the OTM Windows and Web Navigators. They also control access to the Web based Telephone pages.

User Groups are added and deleted in the OTM Windows Navigator.

User Group	Last Modified	Number of Users
Administrators	12/8/2001 3:51:57 PM	1
HelpDesk	12/8/2001 3:53:49 PM	0
EndUser	12/8/2001 4:45:04 PM	1
Default	12/8/2001 3:58:45 PM	0

Applet UserGroupManager.ProfileManager started

Navigator access

Access to the sites, systems, and applications available in both the Windows and Webs is controlled on a user-group basis through the User Group Properties Java application.

When the user group name is entered into the User Group field in an OTM user's directory record, the entry must match the user group name exactly. This is primarily a concern when OTM is operating in a language other than English. In this case, the access profile name "HelpDesk" may have been translated into the local language.

To modify the access rights of a user group:

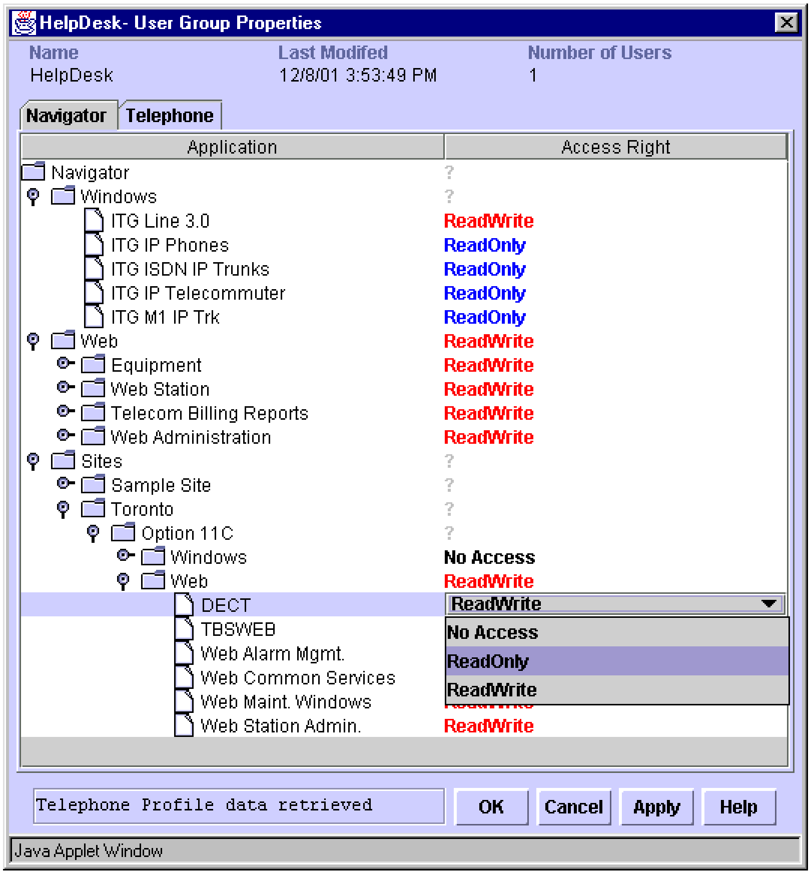
1 Click to select a User Group.

2 Click **Edit**.

The User Group Properties Java application launches, and the User Group Properties dialog box for the selected user group appears. See Figure 92 on page 192.

Alternatively, you can double-click the user group to display the **User Group Properties** dialog box for the selected user group.

Figure 92
User Group Properties dialog box—Navigator tab



HelpDesk- User Group Properties

Name	Last Modifed	Number of Users
HelpDesk	12/8/01 3:53:49 PM	1

Application	Access Right
Navigator	?
Windows	?
ITG Line 3.0	ReadWrite
ITG IP Phones	ReadOnly
ITG ISDN IP Trunks	ReadOnly
ITG IP Telecommuter	ReadOnly
ITG M1 IP Trk	ReadOnly
Web	ReadWrite
Equipment	ReadWrite
Web Station	ReadWrite
Telecom Billing Reports	ReadWrite
Web Administration	ReadWrite
Sites	?
Sample Site	?
Toronto	?
Option 11C	?
Windows	No Access
Web	ReadWrite
DECT	ReadWrite
TBSWEB	
Web Alarm Mgmt.	
Web Common Services	
Web Maint. Windows	
Web Station Admin.	ReadWrite

Telephone Profile data retrieved

The Access Right column lists the level of access allowed for each site, system, and application. This is the same tree structure and performs the same function as the Windows-based New User Group Properties dialog box .

The question mark indicates that the sub-items belonging to the item displaying the question mark have mixed access settings.

To modify access rights:

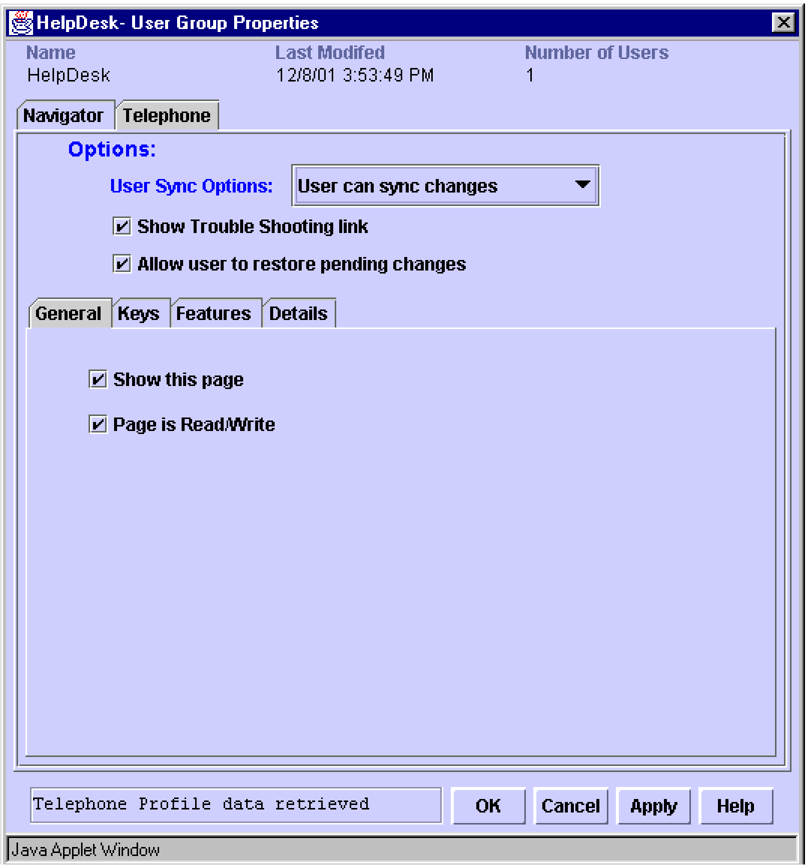
1 Use the drop-down list to select **ReadWrite**, **ReadOnly**, or **No Access** for each item in the tree.

2 Click **Apply**.

Telephone access

The Telephone tab in the User Group Properties dialog box is used to control access to the telephone pages on the web for each user group. See Figure 93.

Figure 93
Telephone access properties dialog box—General Tab



HelpDesk- User Group Properties

Name: HelpDesk
Last Modifed: 12/8/01 3:53:49 PM
Number of Users: 1

Options:

User Sync Options: User can sync changes

☑ Show Trouble Shooting link

☑ Allow user to restore pending changes

☑ Show this page

☑ Page is Read/Write

Telephone Profile data retrieved

The options that are configured in the upper section of this dialog box are applicable to all of the tabs in telephone pages. These options include:

- Allowing or denying this group the ability to synchronize changes with the system. If synchronization is denied, you must manually synchronize the changes with the system using Station Administration.

- Determining whether the troubleshooting link appears at the top of the telephone page for members of this group.
- Allowing or denying this group the ability to restore changes that have been made to a telephone.

Procedure 35
Configuring telephone access options

1 Use the drop-down list to select either **User can sync changes** or **User cannot sync changes**.

2 Select **Show Trouble Shooting link** check box to enable this option.

For EndUsers, clicking the link appears the Telephone Troubleshooting Help page which includes a reset button.

For Web users, clicking the link appears the maintenance page for the telephone with all of the available commands.

3 Select **Allow users to restore pending changes** check box to permit the users in this group to restore the changes made to a telephone.

4 Click **Apply** to apply your changes.

End of Procedure

General tab

In the General tab, you use check boxes to determine whether the Telephone—General page appears for this user group and whether the users in this group are able to make changes to this Telephone page. The Telephone—General page contains information such as site, system, location, and TN, which may not be appropriate for or valuable to end users.

Procedure 36
Configuring the Telephone—General page

1 Select **Show this page** check box to allow this user group to be able to view the Telephone—General page.

2 Select **Page is Read/Write** check box to allow users in this group to make changes to the information that appears in this telephone page.

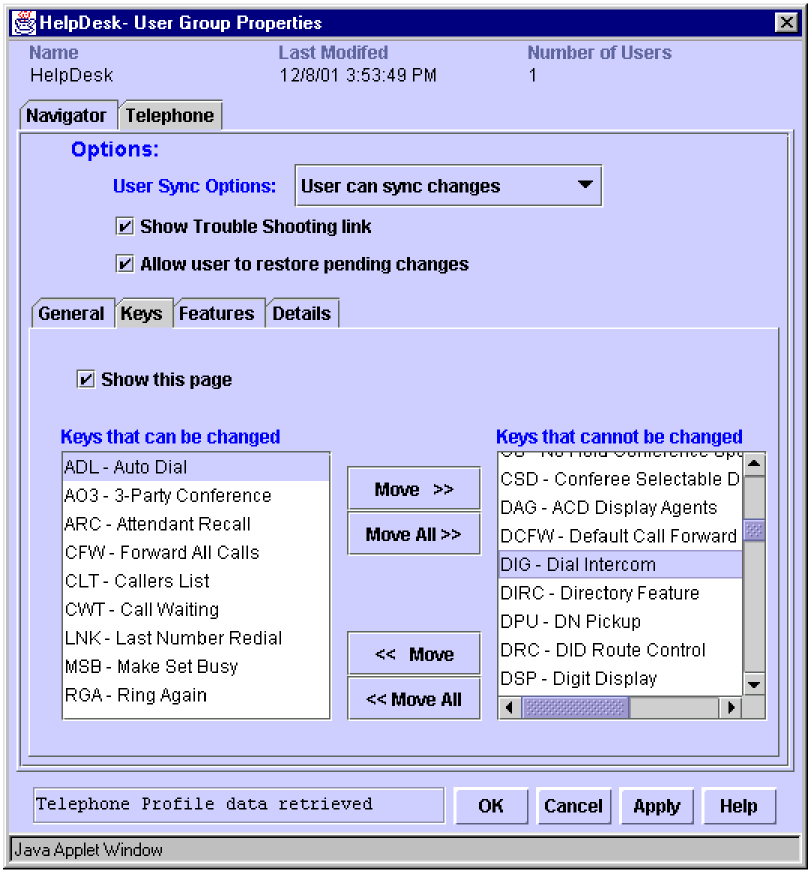
3 Click **Apply** to apply your changes.

End of Procedure

Keys tab

In the Keys tab, see Figure 94, you use the check box and lists of key-based features to determine whether the Telephone—Keys page appears and, if so, which keys the users in this group can change.

Figure 94
Telephone access properties dialog box—Keys tab



HelpDesk- User Group Properties

Name: HelpDesk
Last Modifed: 12/8/01 3:53:49 PM
Number of Users: 1

Options:

User Sync Options: User can sync changes

☑ Show Trouble Shooting link

☑ Allow user to restore pending changes

☑ Show this page

Keys that can be changed

- ADL - Auto Dial
- AO3 - 3-Party Conference
- ARC - Attendant Recall
- CFW - Forward All Calls
- CLT - Callers List
- CWT - Call Waiting
- LNK - Last Number Redial
- MSB - Make Set Busy
- RGA - Ring Again

Keys that cannot be changed

- CSD - Conferee Selectable D
- DAG - ACD Display Agents
- DCFW - Default Call Forward
- DIG - Dial Intercom
- DIRC - Directory Feature
- DPU - DN Pickup
- DRC - DID Route Control
- DSP - Digit Display

Telephone Profile data retrieved

Procedure 37
Configuring the Telephone—Keys page

To configure the Telephone—Keys page:

1. Select the **Show this page** check box to allow this user group to be able to view the Telephone—Keys page.
2. Use the Move and Move All buttons to move the key-based features that this user group can change into the left column.

By putting keys into the left column, users in this group can interchange these key types and change the key parameters.

If the user selects a key that is not in the left-hand column while viewing the Telephone—Keys page, the Change button does not appear.

3 Click **Apply** to apply your changes.

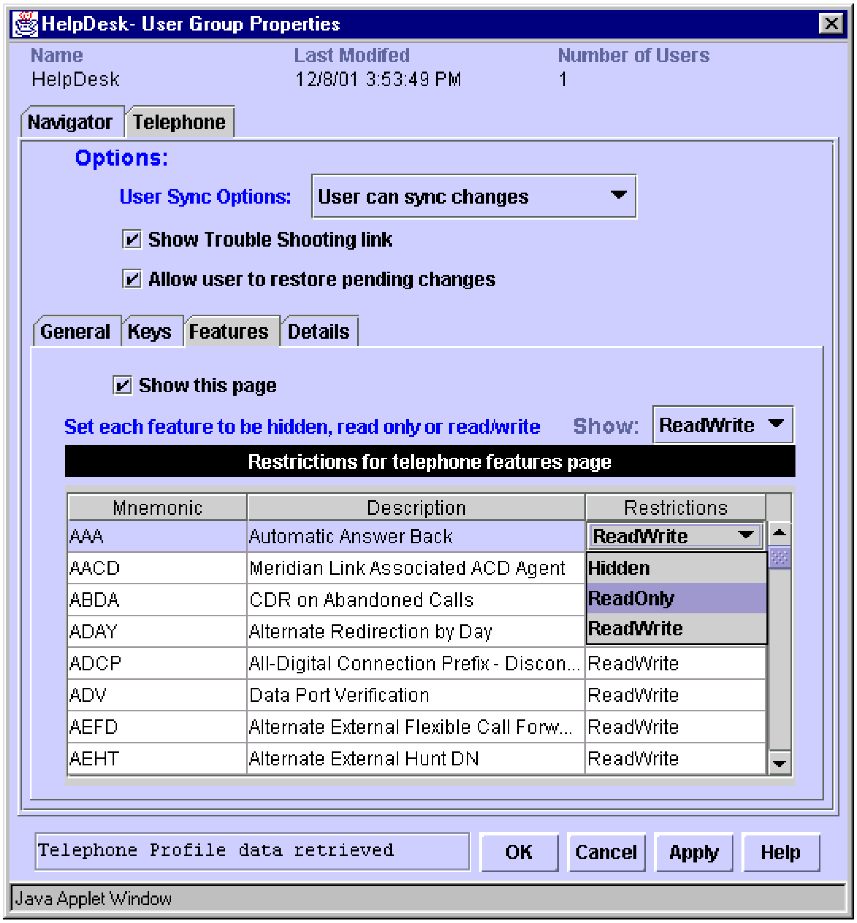
End of Procedure

Features tab

In the Features tab, see Figure 95 on page 197, you use the check box and list of features to determine whether the Telephone—Features page appears and, if so, which features the users in this group can view and change. The list of features contains all the non-key features listed alphabetically by prompt in LD 10 and LD 11. Each feature is assigned a restriction of Hidden, ReadOnly, or ReadWrite. If Hidden, the feature does not appear in the end user Feature drop-down list.

Read/Write capability requires the OTM Premium package.

Figure 95
Telephone access properties dialog box—Features tab



Name: HelpDesk
Last Modifed: 12/8/01 3:53:49 PM
Number of Users: 1

Options:

User Sync Options: User can sync changes

☑ Show Trouble Shooting link

☑ Allow user to restore pending changes

☑ Show this page

Set each feature to be hidden, read only or read/write Show: ReadWrite

Restrictions for telephone features page

Mnemonic	Description	Restrictions
AAA	Automatic Answer Back	ReadWrite
AACD	Meridian Link Associated ACD Agent	Hidden
ABDA	CDR on Abandoned Calls	ReadOnly
ADAY	Alternate Redirection by Day	ReadWrite
ADCP	All-Digital Connection Prefix - Discon...	ReadWrite
ADV	Data Port Verification	ReadWrite
AEFD	Alternate External Flexible Call Forw...	ReadWrite
AEHT	Alternate External Hunt DN	ReadWrite

Telephone Profile data retrieved

Procedure 38
Configuring the Telephone—Features page

To configure the Telephone—Features page:

1 Select **Show this page** check box to allow this user group to be able to view the Telephone—Features page.

Use the drop-down lists in the Restrictions column to configure each feature as ReadWrite, ReadOnly, or Hidden.

The Show drop-down list contains All, Hidden, ReadOnly, and ReadWrite. This is used to limit the size of the list.

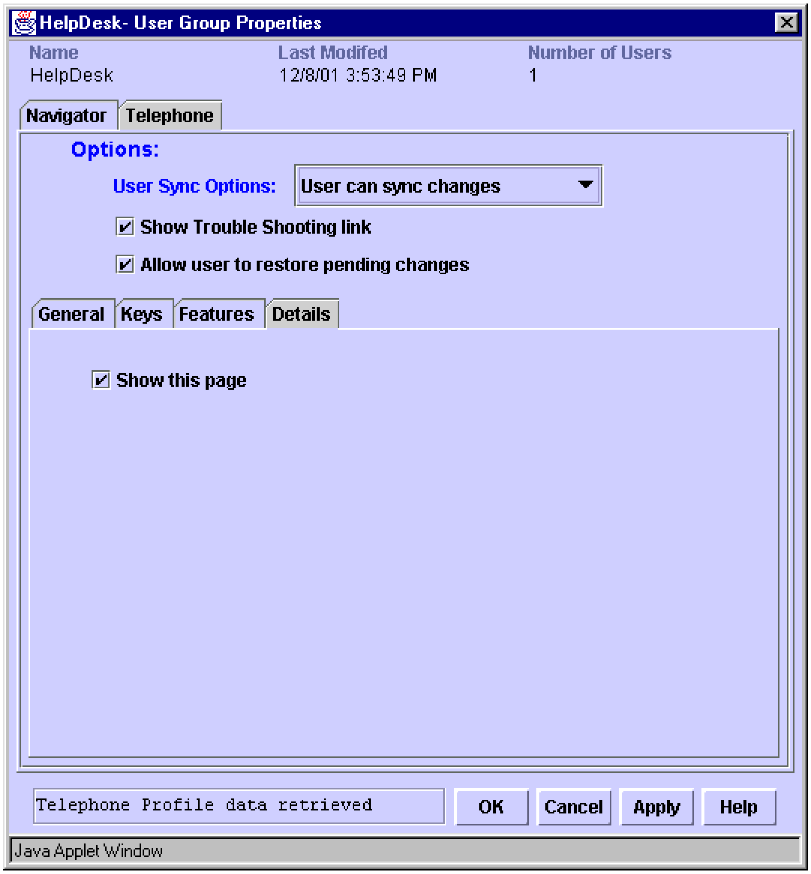
2 Click **Apply** to apply your changes.

End of Procedure

Details tab

In the Details tab, see Figure 96, you use the check box to determine whether the Telephone—Details page appears.

Figure 96
Telephone access properties dialog box—Details tab



HelpDesk- User Group Properties

Name	Last Modifed	Number of Users
HelpDesk	12/8/01 3:53:49 PM	1

Options:

User Sync Options: User can sync changes

☑ Show Trouble Shooting link

☑ Allow user to restore pending changes

☑ Show this page

Telephone Profile data retrieved

Installing and configuring desktop services

Procedure 39
Installing and Configuring Desktop Services

The following procedure outlines the steps that you must take to install and configure Desktop Services.

1 Install OTM. See “Adding OTM web users” on page 183.

2 Create accounts for Help Desk users and End Users as required.

3 Log in to the Web as Administrator, and go to the User Groups page.

To navigate to the Administrator Login page, place **`/admin`** after the OTM IP address or host name in your web browser.

4 Configure the Help Desk, Default, and End User Access Profiles as desired.

By default, Help Desk users are given read/write access to all features. Default and End Users have read-only access to 21 features.

To enable Help Desk users to make changes to other user’s telephone configuration data, make sure that they have access to the Find Telephones page.

5 Enter the Help Desk user’s Login Name and Access Profile in the user’s OTM Directory entry. See “Enable web desktop access in the OTM Directory” on page 199.

6 Enter the End User’s Login Name and Access Profile in the user’s OTM Directory entry. See “Enable web desktop access in the OTM Directory” next.

7 Select the desired web Reporting Role in the user’s OTM Directory entry.

End of Procedure

Enable web desktop access in the OTM Directory

You can give end-users an account on the OTM server using the same process that is used to allow Administrators and HelpDesk users to access the Windows and Webs; however, end-users are typically authenticated through LDAP. End-users do not normally have accounts on the OTM server. When the LDAP authentication method is used, mapping for the following attributes is performed using the OTM Directory:

- Login Name - required to associate users with their telephones
- User Group - determines what users can see and changes that they can make on their telephones
- Web Reporting Access Rights - controls access to web TBS billing reports

Procedure 40
Enabling web desktop access

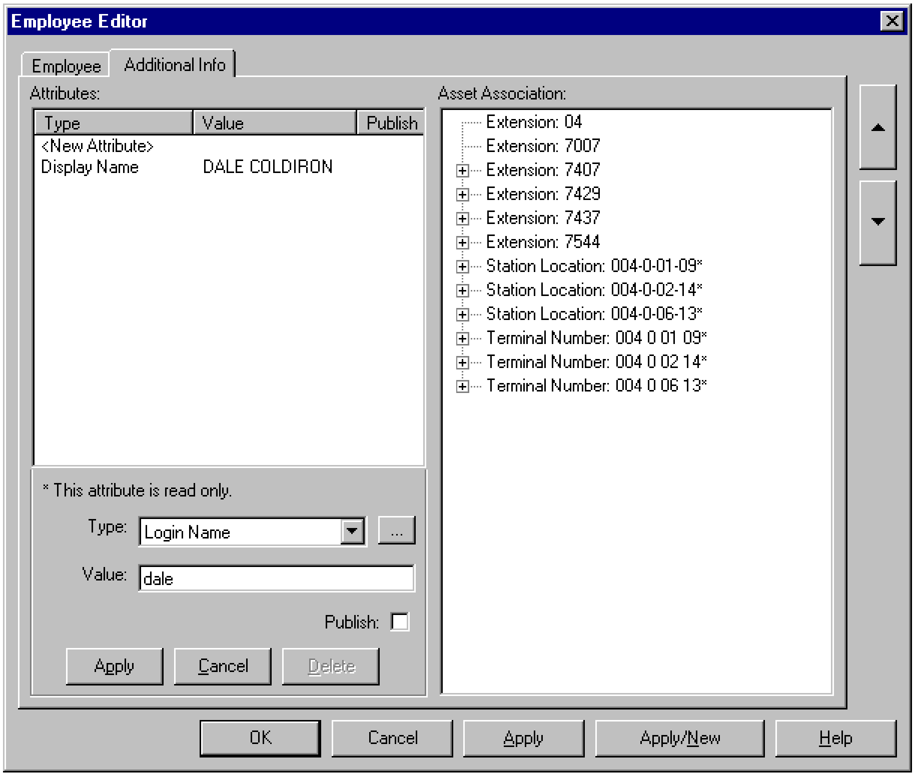
1 From Station Administration, select **View > Employee Selector**.

2 Double-click an employee's name in the **Employee Selector** window.

The Employee Editor window for the selected employee appears.

3 Click the **Additional Info** tab in the Employee Editor window. See Figure 97.

Figure 97
Entering Login Name attribute



Employee Editor

Attributes:

Type	Value	Publish
<New Attribute>		
Display Name	DALE COLDIRON	

* This attribute is read only.

Type: Login Name

Value: dale

Publish: □

Asset Association:

- Extension: 04
- Extension: 7007
- Extension: 7407
- Extension: 7429
- Extension: 7437
- Extension: 7544
- Station Location: 004-0-01-09*
- Station Location: 004-0-02-14*
- Station Location: 004-0-06-13*
- Terminal Number: 004 0 01 09*
- Terminal Number: 004 0 02 14*
- Terminal Number: 004 0 06 13*

4 Select **<New Attribute>** in the Attributes pane.

5 Select **Login Name** from the Type drop-down box.

6 Enter the user's Login Name in the Value field.

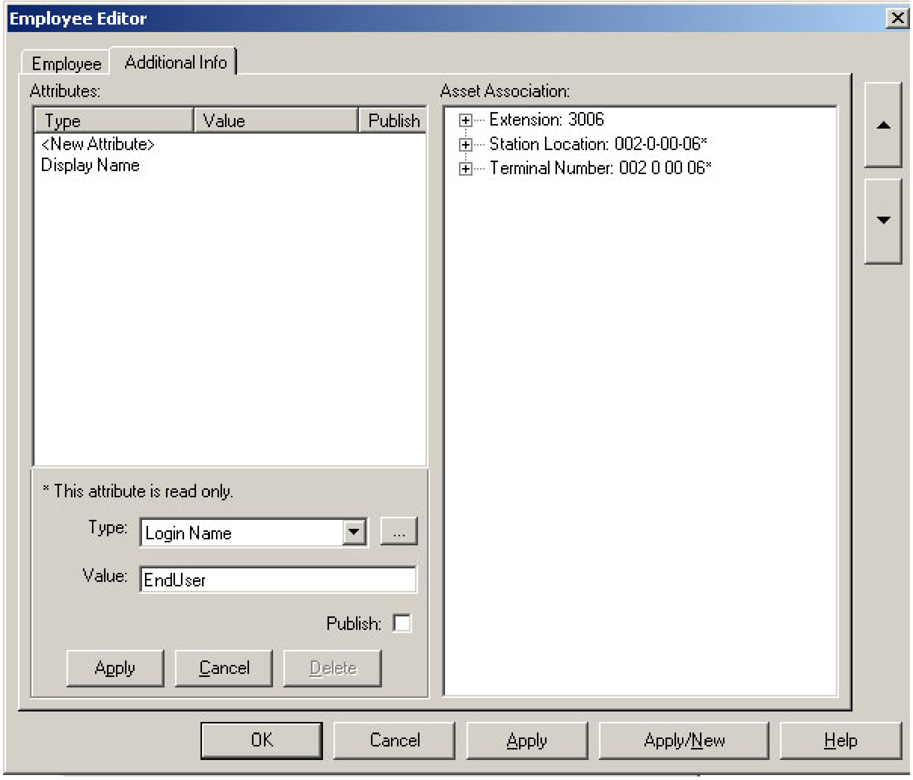
7 Select the **Publish** check box to enable synchronization with an optional LDAP-compliant server.

8 Click **Apply** in the Attributes pane.

9 Select **<New Attribute>** in the Attributes pane.

10 Select **User Group** from the Type drop-down box. See Figure 98.

Figure 98
Entering User Group attribute



Employee Editor

Attributes:

Type	Value	Publish
<New Attribute>		
Display Name		

Asset Association:

Extension: 3006
Station Location: 002-0-00-06*
Terminal Number: 002 0 00 06*

* This attribute is read only.

Type: Login Name

Value: EndUser

Publish: □

11 Select EndUser from the Attributes Value drop-down list to enable End User web desktop user access.

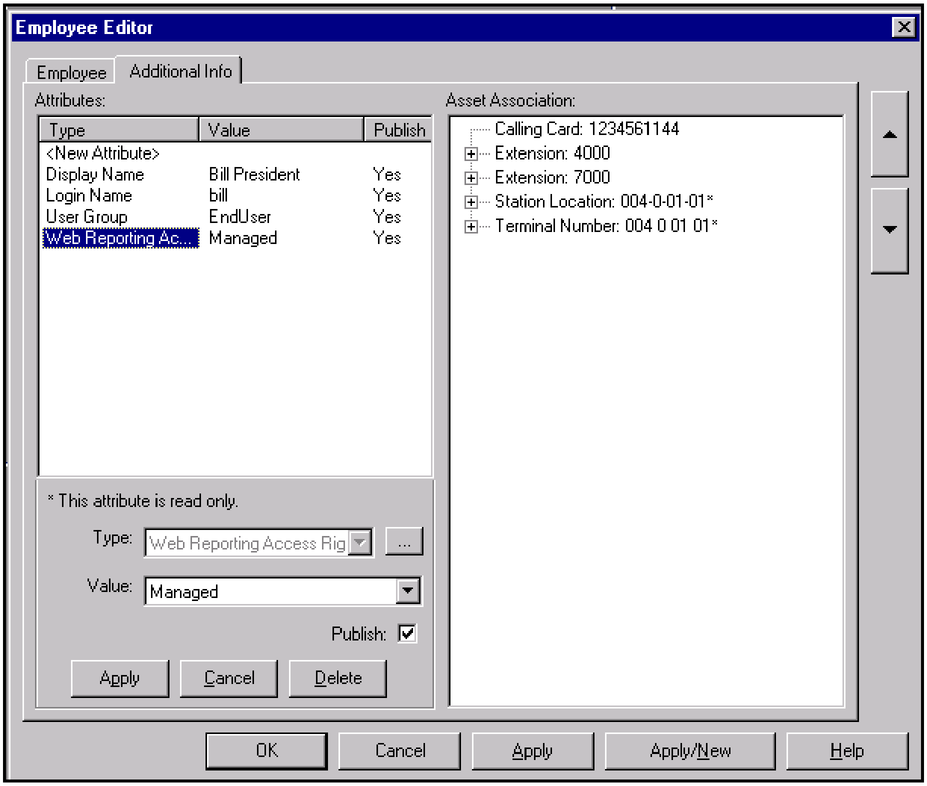
Select HelpDesk from the Attributes Value drop-down list to enable Help Desk web desktop user access.

12 Click **Apply** in the Attributes Pane.

13 Select **<New Attribute>** in the Attributes pane.

14 Select **web Reporting Access Rights** from the Type drop-down box. See Figure 99 on page 202.

Figure 99
Entering web Reporting Access Rights attribute



Employee Editor

Employee | Additional Info

Attributes:

Type	Value	Publish
<New Attribute>		
Display Name	Bill President	Yes
Login Name	bill	Yes
User Group	EndUser	Yes
Web Reporting Ac...	Managed	Yes

* This attribute is read only.

Type: Web Reporting Access Rig

Value: Managed

Publish: ☑

Asset Association:

- Calling Card: 1234561144
- Extension: 4000
- Extension: 7000
- Station Location: 004-0-01-01*
- Terminal Number: 004 0 01 01*

15 Select one of the following access levels for the attribute value:

- All - Users assigned this role have the authority to view all the reports for the site/systems to which they are assigned. This is the access level that you typically assign to an Administrator.
- Peer - Users assigned this role have the authority to view the reports for all the entities in the same node in the Organizational Hierarchy and all its sub-nodes. This is the access level that you typically assign to a person who manages several departments.
- Managed - Users assigned this role have the authority to view their own reports and the reports for all of the entities in the sub-nodes below their organization

node in the Organizational Hierarchy. This is the access level that you typically assign to a department manager.

- Personal - Users assigned this role have the authority to view their own data. This is the access level that you assign to a non-managerial employee.
- No Access - If no role is assigned for a user, their reporting access rights default to No Access.

End of Procedure

For Desktop User Groups, you can use the Directory Update page in the OTM webOTM Web Navigator to simplify this process. See “Web Services” in *Optivity Telephony Manager: System Administration* (553-3001-330).

If you have access to the Login Names in another database, consider using the Import/ Export utility in the OTM System Window to simplify this process. See “Import and Export Utilities” in *Optivity Telephony Manager: System Administration* (553-3001-330).

“Appendix A” in *Optivity Telephony Manager: System Administration* (553-3001-330) contains end-user reference information. You can extract this appendix and distribute it as a user guide.

Setting up the LDAP server

This chapter contains information on how the LDAP server utility allows you to link and synchronize the OTM and Corporate LDAP databases. OTM acts as an LDAP client to the Corporate LDAP server database.

You can use the LDAP server to link an employee entry in the OTM directory to an entry in the LDAP directory. If employee data exists in the LDAP directory, you can select and add the employee entry into the OTM directory; or if the employee entry resides in both directories, you can select and link the entry.

When you link an entry between the OTM directory and the LDAP directory, OTM updates the entry's attribute data when you synchronize the directories. The following are examples of LDAP attributes:

- first name
- last name
- department
- telephone extension

Scheduled synchronizations only synchronize OTM directory entries that have their Publish check box selected. Synchronization only compares and updates entries that have the same Unique Identifier (UID) in both the OTM directory and the LDAP-compliant server. You can use the LDAP Synchronization Utility or the Import and Export Utility to manually set up the UID.

> ***Note:*** The UID in OTM is a string and cannot be mapped to the GUID field of Novell NDS.

For detailed instructions on setting up the LDAP server, as well as an example of importing attributes to the OTM directory, see *LDAP Synchronization* in *Optivity Telephony Manager: System Administration* (553-3001-330).

For information on importing non-LDAP-compliant directory information into the OTM directory, see *Import and Export Utilities* in *Optivity Telephony Manager: System Administration* (553-3001-330).

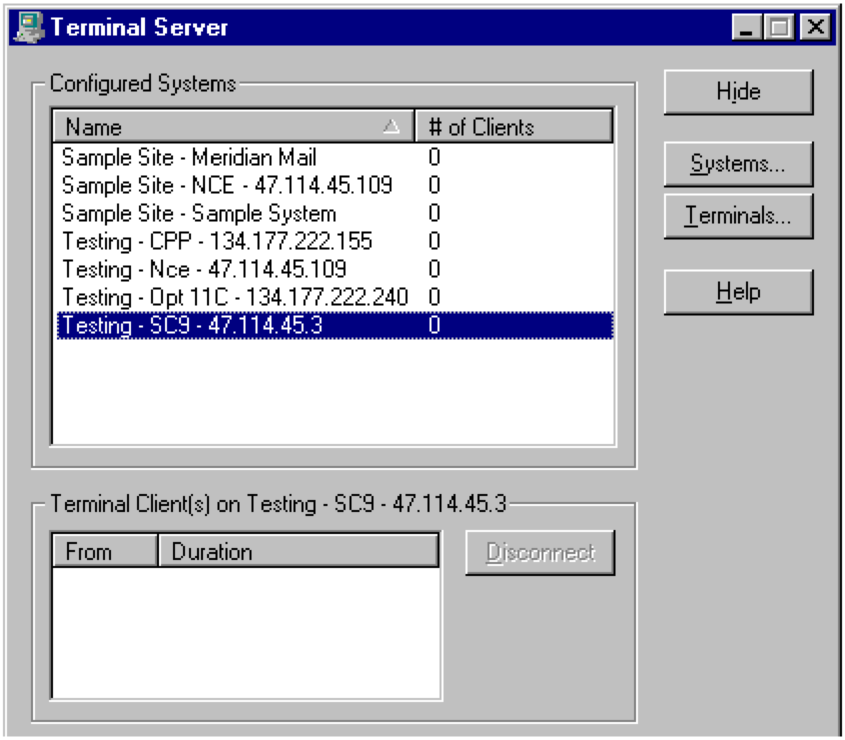
Terminal server

The Terminal server application is a Windows application that uses the OTM database to obtain site, system, and IP address information. The Terminal server supports direct serial connections and system overlay connection over an IP network. If you connect over an IP network to a system, you can customize the port user types (SCH, MTC, BUG, TRF).

Terminal server setup

To launch the Terminal server application, from the Start menu, select **Programs > Optivity Telephony Manager > Terminal server**. The Terminal server dialog box opens. See Figure 100.

Figure 100
Terminal server dialog box



Name	# of Clients
Sample Site - Meridian Mail	0
Sample Site - NCE - 47.114.45.109	0
Sample Site - Sample System	0
Testing - CPP - 134.177.222.155	0
Testing - Nce - 47.114.45.109	0
Testing - Opt 11C - 134.177.222.240	0
Testing - SC9 - 47.114.45.3	0

Terminal Client(s) on Testing - SC9 - 47.114.45.3

From	Duration

IMPORTANT!

Click **Hide** on **Terminal server** dialog box (see Figure 100 on page 207), **do not** close from the window **close** button ("X") as this loses all configuration.

The Terminal server window appears two lists:

- configured systems
- configured ports

The configured systems list appears information on the virtual port that is configured:

- Name:
  As defined in the OTM Windows Navigator
- Number of clients:
  The number of terminal clients using the port

When you select an entry in the Configured Ports list, the clients on Port list appears the following information for each terminal client using the port:

- From:
  IP address of the terminal client
- Duration:
  How long the connection has been in use

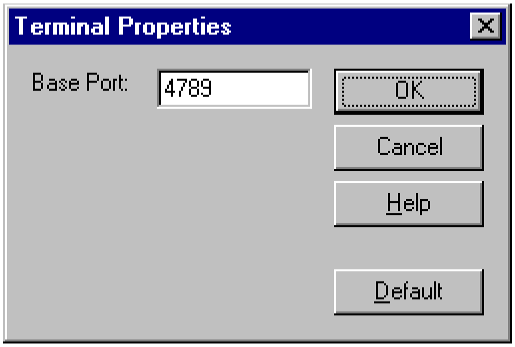
The Disconnect button next to the clients on Port list allows you to terminate the connection to one or more terminal clients.

The Terminal server application also has the following buttons:

- **Hide** Hides the application window. During normal operation, the Terminal server application runs without user input, so hiding its window frees up some desktop space. You can view the window at any time by double-clicking the Terminal Service icon in the Task Bar tray.
- **Systems...** Configures the virtual ports. See "Virtual ports" on page 209" .

- **Terminals...** Configures the starting network socket port number for communications between the OTM server and the OTM web System Terminal see Figure 101 on page 209. The default is 4789. Typically, you will not need to change this.
- **Help** Get context-sensitive Help on the application.

Figure 101
Terminal Properties dialog box



Terminal Properties

Base Port: 4789

Virtual ports

In the Terminal server application, the Virtual Ports Properties window allows you to enable or disable connection to a particular device. It appears the virtual port number for each configured device, and the corresponding serial or network settings.

In the Virtual Port Properties window, a tree appears the devices that can be connected via a virtual port. For serial ports, the window retrieves the available serial ports from the Registry. For network connections, the window retrieves the site and system information from the OTM database. The virtual port for a system uses the same IP address assigned to System Terminal. The tree mirrors the tree in the OTM Navigator. It uses the communication profile in System Properties, determined as follows:

- For a Generic system, it uses the profile (serial or network) selected in the Application page in System Properties.
- For a non-Generic system, it uses the communication settings from the profile (serial or network) assigned to VT220 in the Applications page in System Properties.
- For any system, if a network (Ethernet) profile is selected, Terminal server uses a Telnet connection.

To configure virtual port connection for a device, click Systems in the Terminal server window, or double-click a Configured System in the list (this selects the corresponding device in the Virtual Port Properties window allowing you to quickly change the settings for a particular device).

To enable virtual port connection for a device, do one of the following:

- Double-click the disabled port in the tree.
- Select the item and select the Enabled check box.
- Click **Enable All**. This enables all the items listed in the tree with the default configuration. The item becomes bold to show that it is enabled.

The field to the right of the Enabled check box automatically fills in the Site - System name for the selected device. This is the name displayed in the Terminal server's main window.

To disable a virtual port, do one of the following:

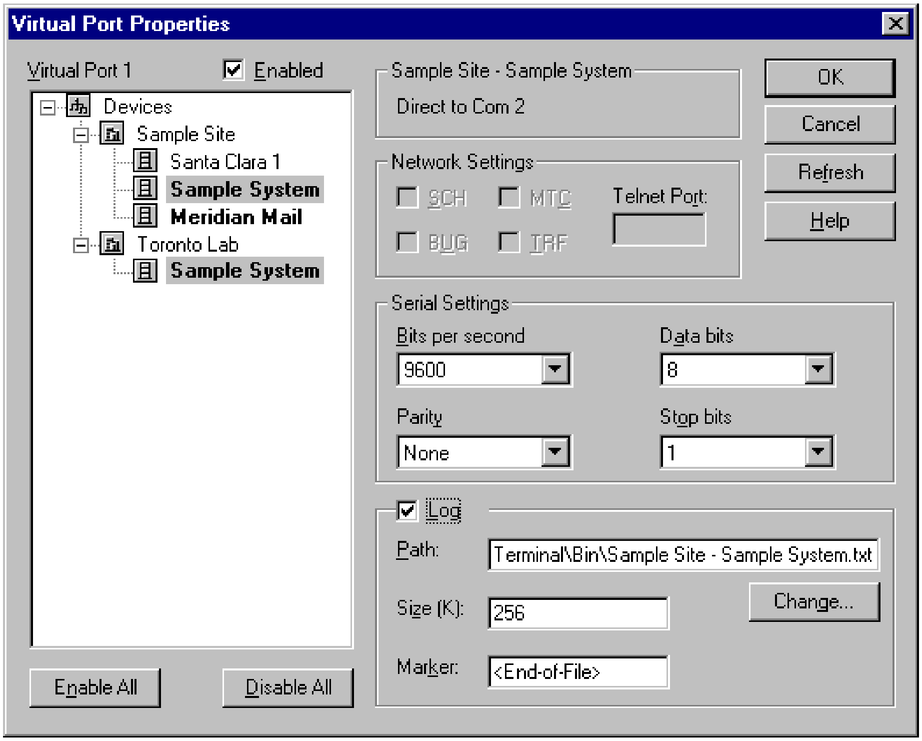
- Double-click an enabled item in the tree.
- Select the item and clear the Enabled check box.
- Click **Disable All.** This disables all the devices listed in the tree. The item is no longer bold, and does not appear from the Terminal server main window when you click **OK**.

Serial connections

The Terminal server application supports all the serial ports on the OTM server PC plus the systems configured in the OTM Navigator. However, while more than 8 serial ports may be configured, the Terminal server is limited to 8 simultaneous serial connections. (The limit depends on the OTM server hardware, the network capacity, the server's CPU capacity, and so on.)

For a serial connection, Direct to Com x appears, where x is the com port number. The fields for serial settings are enabled. The default is the serial settings from the OTM database. You can change the settings in the dialog box as shown Figure 102 on page 211.

Figure 102
Virtual Port Properties (Serial with Logging enabled)



Virtual Port 1 ☑ Enabled

Sample Site - Sample System
Direct to Com 2

Network Settings
□ SCH □ MTC □ BUG □ TRF
Telnet Port:

Serial Settings
Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1

☑ Log
Path: Terminal\Bin\Sample Site - Sample System.txt
Size (K): 256
Marker: <End-of-File>

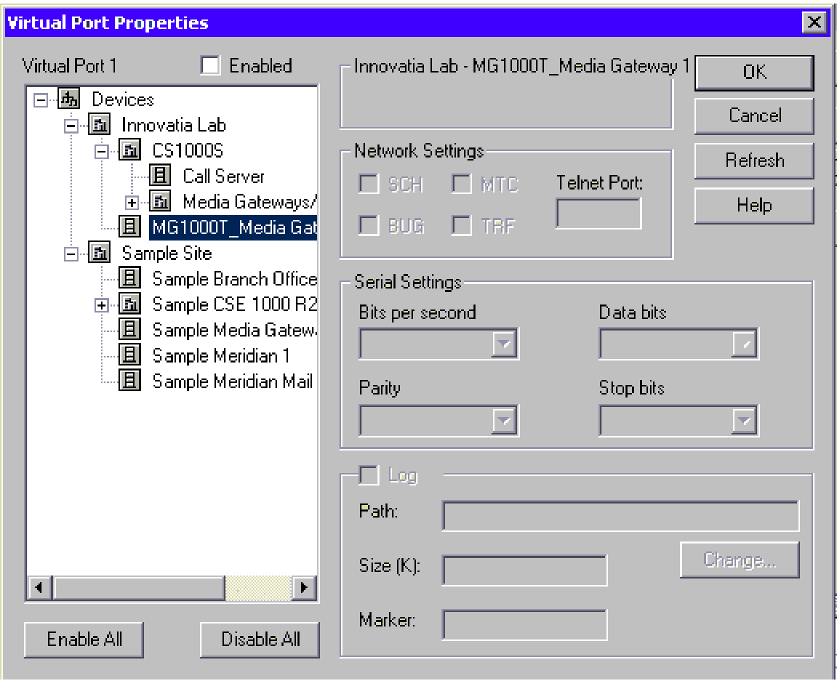
Network connections

For a network connection, the IP address appears. It also indicates whether the system is a Meridian 1, CS 1000, or Generic.

- Make sure the IP address is correct. If the IP address is different from the OTM database’s setting, click Refresh to update all of the network ports with the latest settings from the OTM database.
- If you select an M1 or CS 1000 System, the fields for M1 port settings are enabled (default = SCH). The Telnet port field is disabled.
- If you select a Generic System, the fields for both serial and M1 port settings are disabled. The Telnet port field is enabled.

- Select the Log check box to turn on data capture. The log file name defaults to the Site - System name plus a .txt extension. The path and the file name can be changed by typing in the edit box or clicking Change.
- The maximum size of the log file is customizes (in the Size field) on a per-system basis, and defaults to 256 K. Once the file size reaches the limit, the Terminal server starts from the beginning of the file, overwriting the oldest logs.
- Due to the circular nature of the log, the Terminal server writes an end-of-file marker (customizes in the Marker field) at the end of the log entries.
- The log records the time and date of when a client connects and disconnects to the virtual port, and writes all text received from and sent to the host. This allows a network administrator to keep an activity log of the virtual port connection.
- If this ASCII log is to be viewed from a web browser, the file should be stored in a web-accessible path.Virtual Port Properties (Network with Logging disabled) See Figure 103.

Figure 103
Virtual Port Properties (Network with Logging disabled)



Configuring the web browser client

This chapter contains information on configuring the OTM web browser client.

Make sure that the PC client requirements have been met, as described in "OTM hardware requirements" on page 39.

Configure Windows® XP SP2 to work with OTM

Procedure 41
Configure Windows XP SP2 to work with OTM

1 Open **Control Panel > Internet Connection Firewall** . Choose one of the following options:

   a. **Select General** Tab, then set **Internet Connection Firewall** to "Off" Mode, or

   b. Select **Exceptions**, then select only those applications that you want network access enabled.

2 To enable web applications from the Internet Explorer menu bar, select **View** > **Manage Add-Ons** > then select **Add-ons that have used by Internet Explorer** and enable all.

3 From the Internet Explorer menu bar, select **Tools > Pop-Up Manager** > then enable Pop-Up Windows.

4 From the Internet Explorer menu bar, **Tools** > **Internet Options** > **Security** > **Trusted Sites** > click **Sites** > then add server IP address to trusted site.

End of Procedure

Accessing the OTM server Web using the PC client

Procedure 42
Accessing the OTM server Web using the PC client

1 Enter the OTM server IP address or computer name in the location bar of the web browser on the PC client.

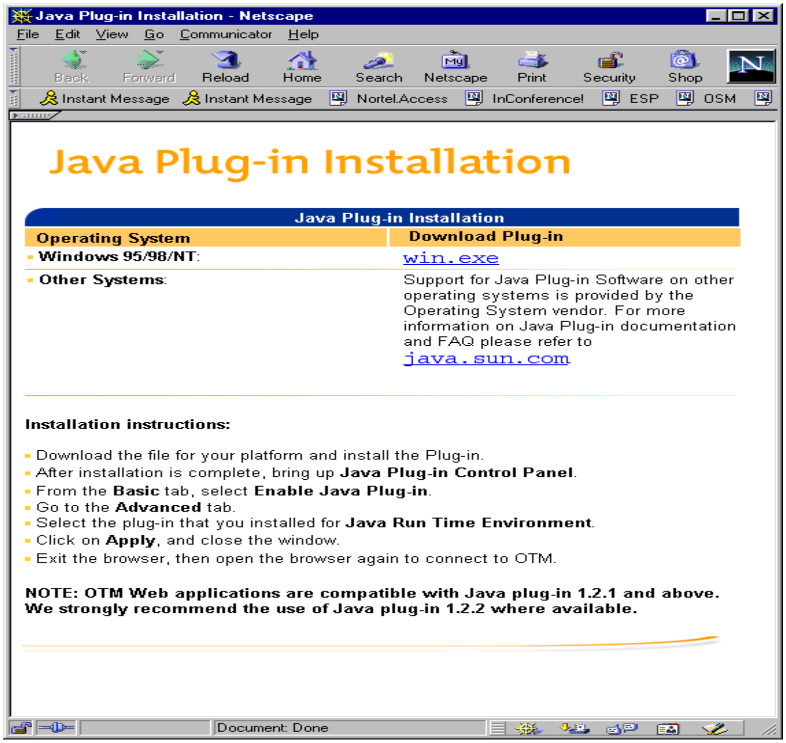
2 Press **Enter**.

End of Procedure

Software plug-in

The first time the OTM server Web loads, you are prompted to download a software plug-in. See Figure 104. The software you download is a standard Java Runtime Environment (JRE) plug-in of about 7-8 MB size.

Figure 104
JRE Plug-in download prompt


Java Plug-in Installation - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop
Instant Message Instant Message Nortel.Access InConference! ESP OSM
Document: Done

Java Plug-in Installation

Java Plug-in Installation	
Operating System	**Download Plug-in**
Windows 95/98/NT:	win.exe
Other Systems:	Support for Java Plug-in Software on other operating systems is provided by the Operating System vendor. For more information on Java Plug-in documentation and FAQ please refer to java.sun.com

Installation instructions:

- Download the file for your platform and install the Plug-in.
- After installation is complete, bring up **Java Plug-in Control Panel**.
- From the **Basic** tab, select **Enable Java Plug-in**.
- Go to the **Advanced** tab.
- Select the plug-in that you installed for **Java Run Time Environment**.
- Click on **Apply**, and close the window.
- Exit the browser, then open the browser again to connect to OTM.

NOTE: OTM Web applications are compatible with Java plug-in 1.2.1 and above. We strongly recommend the use of Java plug-in 1.2.2 where available.

Integrating OTM with Optivity NMS

Contents

This chapter contains information on the following topics:

Overview

Optivity Telephony Manager (OTM) integrates with Optivity Network Management System (NMS) versions 10.1 and 10.2. Optivity NMS is an enterprise-level network management solution providing fault, performance, configuration, and security management for Nortel inter-networking devices. Through Optivity NMS, you can monitor your OTM servers.

OTM Alarm Manager receives SNMP traps from managed CS 1000 and Meridian 1 entities. Through Alarm Notification, OTM sends filtered traps to Optivity NMS.

By using Optivity NMS InfoCenter, you can manually add OTM servers into the Telephony Managers Resources folder. Property information that you add about the

OTM servers is added to the Optivity NMS database. For access to Optivity NMS documentation, in your web browser go to http://www.nortel.com/documentation. Choose Optivity NMS in the Select a Product drop-down list, and click **View Documents**.

InfoCenter graphically identifies when a device is in an alarm state. By using Optivity InfoCenter, you can set the color for alarm levels. When a device is in an alarm state, you can right-click it to open anOptivity NMS fault management application. For instance, you can start Fault Summary that graphically lists faults for the selected device. You can also set the fault management categories for alarm monitoring.

Integration requirements

This section lists the conditions upon which OTM integrates with Optivity NMS optimally:

- For optimum performance, install OTM on a separate computer from Optivity NMS.
- For more information refer to the OIT support website at http://support.nortel.com. See “Downloading the OIT files” on page 217 for details.
- OTM integrates with Optivity NMS through OIT on any NMS platform. See “Checklist for installing the Optivity Integration Toolkit” on page 218. Co-residence with Optivity NMS, however, is supported only on Windows 2000 server.
- All software requirements for OTM must be met. Install IIS before applying the service pack.
- Always install Optivity NMS prior to installing OTM.

  There are certain restrictions in OTM application features when installed coresident with Optivity NMS.
- Optivity NMS and OTM use different web servers: Apache and IIS respectively.

  In the OTM installation, when installing IIS, make sure that the default HTTP port 80 is not used by both the Apache and the IIS web servers.
- Change the Optivity NMS Apache web server HTTP port from the default value of 80 prior to running IIS installation. If a port clash occurs, the default port on the Apache server must be changed.

OTM– Optivity NMS integration

OTM does not automatically install any OIT files. You must manually install the OIT files. The OIT files can be downloaded from the OIT support web page.

Procedure 43
Downloading the OIT files

To download the OIT files:

1. In your web browser, go to http://support.nortel.com.
2. Click the Product link.
3. In the drop-down list, select **Optivity NMS OIT**, and click **Save**.
4. In the drop-down list for software types, select **Optivity NMS OIT for Optivity Telephony Manager**.
5. Click the link under the Description heading that matches your operating system platform.
6. Click the link to the Readme file to view the installation instructions in your web browser. This file is also included in the zipped archive.
7. Click the link to the zipped archive to download the latest OTM OIT files.

End of Procedure

Integration with ONMS version 10.0

ONMS version 10.0 comes pre-installed with the device OIT files required for releases of OTM prior to OTM 2.0. You must download and install the device OIT file for OTM 2.0 and the application OIT file manually. The application OIT file is common to all releases of OTM. These OIT files can be obtained from the OIT support web page. See “Downloading the OIT files” on page 217 for details.

OTM OIT files

OTM 2.0 requires the following OIT files for integration with ONMS:

- NMS_otm_v10-B.oit
  - OTM server device support entries
  - OTM Open Alarm II definitions
- NMS_otmApp_v10-B.oit
  - OTM web Application integration entries

— OTM also contains the following mib file:

- rfc1223.mib

  — Standard RFC 12313 MIB definitions

Run oitInstall for each .oit file, one at a time. The .mib file must be present in the same directory when oitInstall is executed. See step 5 under "Checklist for installing the Optivity Integration Toolkit."

Checklist for installing the Optivity Integration Toolkit

This section provides general information on OIT. Refer to the NTPs, release notes, and read me files that are provided with your Optivity NMS software package for specific information on OIT.

You can install OIT files for OTM on any platform that runs Optivity NMS as long as it supports the Java Runtime Environment required by OTM web applications (JRE 1.4.2). In this case, follow the steps in this section.

In the case of co-residence, you must understand the prerequisites and install OTM. OTM installation takes automatically performs the OIT integration steps. Steps 1 through 6, as shown in Procedure 44, are then not required.

Checklist for an OTM installation on an existing Optivity NMS server

Procedure 44
Checking the current configuration

1 Log in to Optivity NMS as Administrator.

2 Check for the environment variable LNMSHOME.

View environment variables using the System option in Control Panel on the Environment Variables tab. This variable holds the path of the Optivity installation (typically, c:\Optivity\NMS). All the executables are located in c:\Optivity\NMS\bin.

3 Check for the environment variable OITHOME.

This environment variable points to the Optivity Integration Toolkit home directory (typically, C:\Optivity\oit). If you cannot find OITHOME, create it.

4 Copy OTM OIT files to the appropriate subdirectories in OITHOME.

All of the subdirectories under \Optivity\Oit\ on the OTM CD-ROM are copied to OITHOME.

5 Run LNMSHOME\bin\oitinstall -*u* <*full path of OTM OIT file*> for every .oit file in the OTM directory, where -*u* indicates to upgrade Optivity NMS. If you do not specify the -*u* parameter, only a syntax check is performed on the OIT file.

This command updates the Optivity NMS database with the new definitions.

6 Proceed with OTM installation, checking for prerequisites (IIS, for instance) as always.

End of Procedure

About oitInstall

Optivity NMS includes a program, oitInstall, that extracts the information that Optivity NMS needs for new device application support.

This information includes:

- database schema definitions
- MIB information
- trap information
- device management application launch points from within Optivity NMS applications
- device discovery information

OIT definitions for OTM reside in $OITHOME\OTM\otm.oit. It also contains the file rfc1213.mib.

The $OITHOME environment variable is typically C:\Optivity\oit on Windows systems, and /usr/oit on UNIX.

What you do

OIT definitions are updated into Optivity NMS by manually placing the OIT files into the appropriate directories and starting oitInstall from the command line.

For OTM, you must manually add the OTM server.

What OIT does

The oitInstall program does the following:

- Automatically stops and restarts all Optivity NMS daemons (UNIX) or services (Windows).

- Automatically backs up the Optivity NMS databases, by default /usr/oit/oitdb for UNIX, and C:\Optivity\oit\oitdb for Windows. The oitInstall program automatically restores the database if the device support upgrade installation fails.
- Updates Optivity NMS with two new files: new device and device management support, and deletes the database backup if the integration is successful.

Using Optivity NMS InfoCenter

Once OTM is integrated with Optivity NMS and the OIT definition files, you must manually add OTM server objects to the resources folders in InfoCenter. The OTM integration does not currently support Autodiscovery of these objects.

You must be logged in as administrator/root to perform this activity.

Configuring Optivity NMS InfoCenter for OTM

Procedure 45
Configuring Optivity NMS InfoCenter for OTM

1 Create a Voice Management folder in InfoCenter to contain all of the Voice Elements integrated into Optivity NMS (OTM in this case).

2 Modify the default Properties of the Voice Management folder to display the Optivity Telephony Manager objects added to this folder:

a. Right-click the Voice Management folder and choose **Properties.** See Figure 105 on page 221.

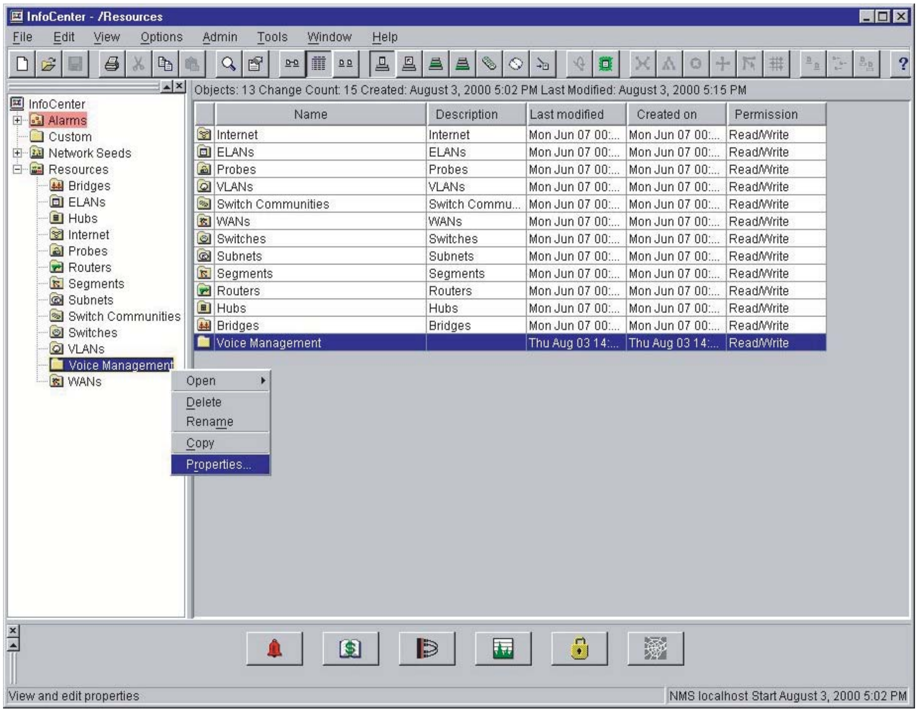
b. Open the Management server folder.

c. Select Optivity Telephony Manager. See Figure 106 on page 222.

d. Click **Apply**.

The wizards provided in Optivity NMS 9.0.1 and later add new OTM servers to Optivity NMS. These wizards automatically establish the Device-Agent-Interface relationship in Optivity NMS databases.

Figure 105
InfoCenter Resources



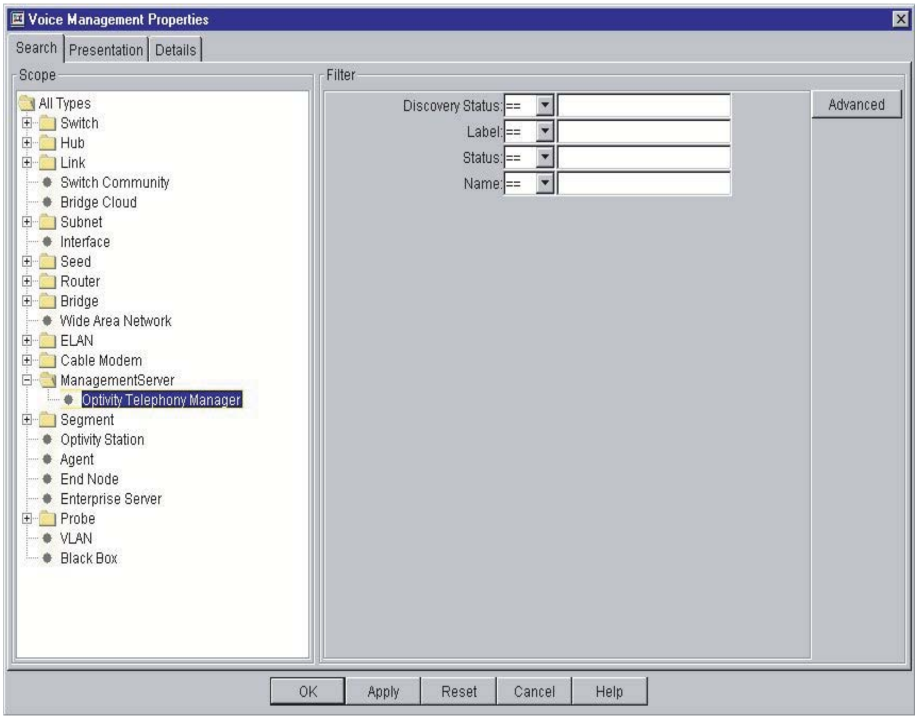
Objects: 13 Change Count: 15 Created: August 3, 2000 5:02 PM Last Modified: August 3, 2000 5:15 PM

Name	Description	Last modified	Created on	Permission
Internet	Internet	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
ELANs	ELANs	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Probes	Probes	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
VLANs	VLANs	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Switch Communities	Switch Commu...	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
WANs	WANs	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Switches	Switches	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Subnets	Subnets	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Segments	Segments	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Routers	Routers	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Hubs	Hubs	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Bridges	Bridges	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Voice Management		Thu Aug 03 14:...	Thu Aug 03 14:...	Read/Write

View and edit properties

NMS localhost Start August 3, 2000 5:02 PM

Figure 106
InfoCenter Voice Management Properties dialog box



Adding OTM server object to Optivity NMS InfoCenter

Add an OTM server resource for every OTM server that you integrate and monitor with Optivity NMS.

If Access Control is enabled, you must have a valid local user account (user name and password) and an Optivity NMS user account to log in to InfoCenter.

Procedure 46
Logging in to InfoCenter

1 From the Windows Start menu, choose **Programs > Optivity > InfoCenter.**

The Optivity NMS InfoCenter login window appears.

2 Type your user name, password, and the name of the Optivity NMS server, and then click **OK**.

Optivity NMS InfoCenter appears.

3 In the Folders pane, click the InfoCenter icon.

4 Double-click the **Resources** folder to open it.

5 A Telephony Managers folder appears.

A Telephony Managers folder is created in Optivity NMS InfoCenter to contain all the Voice Elements integrated into Optivity NMS.

6 Double-click the **Telephony Managers** folder to open it.

7 Modify the default view properties of the folder or you cannot view the OTM servers that are added to this folder.

Right-click the **Telephony Managers** folder and choose **Properties**. Open the Management server folder. Select **Optivity Telephony Manager**, and click **Apply**.

8 From the InfoCenter menu bar, choose **File > New > Object**.

The Object Properties dialog box appears with the Device tab selected. See Figure 107 on page 224.

a. In the Label box, type a label for the new object.

b. In the Type box, select the Management servers object type.

c. In the Subtype box, select an Optivity Telephony Manager subtype for the object.

d. In the IP address box, type the IP address of the object.

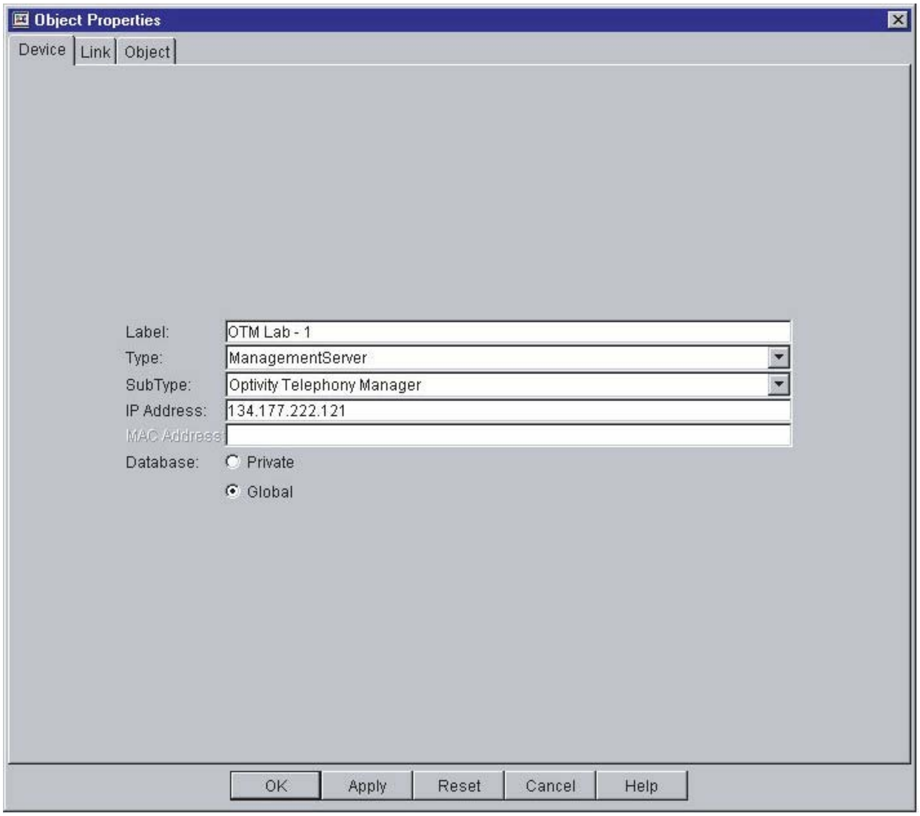
e. Click **Private** or **Global**.

Private lets the local user see the device. Global lets all users see the new object.

f. Click **OK**.

A default switch icon appears for the OTM server.

Figure 107
InfoCenter Object Properties dialog box



Label: OTM Lab - 1

Type: ManagementServer

SubType: Optivity Telephony Manager

IP Address: 134.177.222.121

MAC Address:

Database: ○ Private ● Global

Viewing OTM server object properties

Procedure 47
Viewing OTM server Object Properties

Follow these steps to view the properties of an OTM server in InfoCenter.

1 In InfoCenter, open a folder in the Folders pane.

2 Select the OTM server that you added.

3 From the InfoCenter menu bar, select **File > Properties**.

The Object Properties dialog box appears, displaying the properties for the selected network object. Click **OK**.

End of Procedure

Modifying OTM server object properties

Procedure 48
Modifying OTM server Object Properties

Follow these steps to modify the properties of an OTM server in InfoCenter:

1. In InfoCenter, open a folder in the Folders pane.
2. Select the OTM server that you added.
3. From the InfoCenter menu bar, select **File > Properties**.

   The Object Properties dialog box appears, displaying the properties for the selected network object.
4. Edit the object properties that you want. Click **OK**.

End of Procedure

Starting OTM web applications

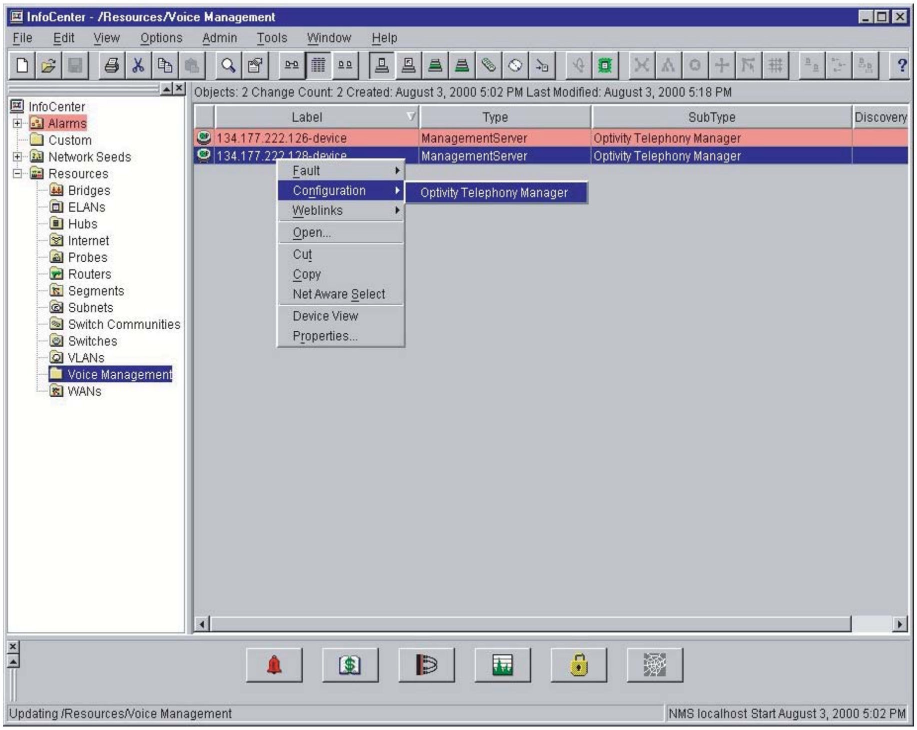
OTM web Application links are integrated with Optivity NMS when an OTM server is added.

The OTM system being accessed can be connected remotely through the network.

You can start OTM web applications by choosing Configuration and selecting Optivity Telephony Manager from the shortcut menu on the OTM icon in Optivity NMS InfoCenter. See Figure 108 on page 226.

This action launches the default web browser for your system and connects to the OTM web server. See “Java Runtime Environment for OTM and Optivity NMS” on page 226 for details on JRE.

Figure 108
Starting OTM web applications



Objects: 2 Change Count: 2 Created: August 3, 2000 5:02 PM Last Modified: August 3, 2000 5:18 PM

Label	Type	SubType	Discovery
134.177.222.126-device	ManagementServer	Optivity Telephony Manager	
134.177.222.128-device	ManagementServer	Optivity Telephony Manager	

Updating /Resources/Voice Management

NMS localhost Start August 3, 2000 5:02 PM

Java Runtime Environment for OTM and Optivity NMS

OTM web applications require Java Plug-In 1.4.2 on the client browser. Optivity NMS uses JDK 1.1.x, which is older than the version used by OTM.

JRE clash for OTM and Optivity NMS web clients

In both coresident and non-coresident situations, OTM and Optivity NMS applications cannot be launched simultaneously. The successful launch of OTM and Optivity NMS web applications accessing JRE depends on the version of JRE currently loaded in the system.

If a version of JRE that is different than 1.4.2 is loaded in the system and you access OTM web applications, you are prompted to install and load Java Plug-In 1.4.2 the first time that you try to connect to the OTM server. With the Java Plug-In 1.4.2 loaded, OTM web applications load successfully.

If a version of JRE that is higher than 1.2.2 is loaded on the system, then Optivity NMS web applications that require JRE cannot be launched. This may occur even when the lower version is installed, but not loaded, on the system. To successfully launch Optivity NMS web applications, you must remove the higher version of JRE, and run the JRE 1.2.2 set-up program.

web server

Optivity NMS uses Apache web server for its web applications, whereas OTM uses Internet Information server (IIS).

Using FaultSummary

OTM filters and then forwards system traps to Optivity NMS. Since OTM forms the main representative agent for systems, all alarms received by Optivity NMS result in the change of status state of OTM depicted in Optivity InfoCenter.

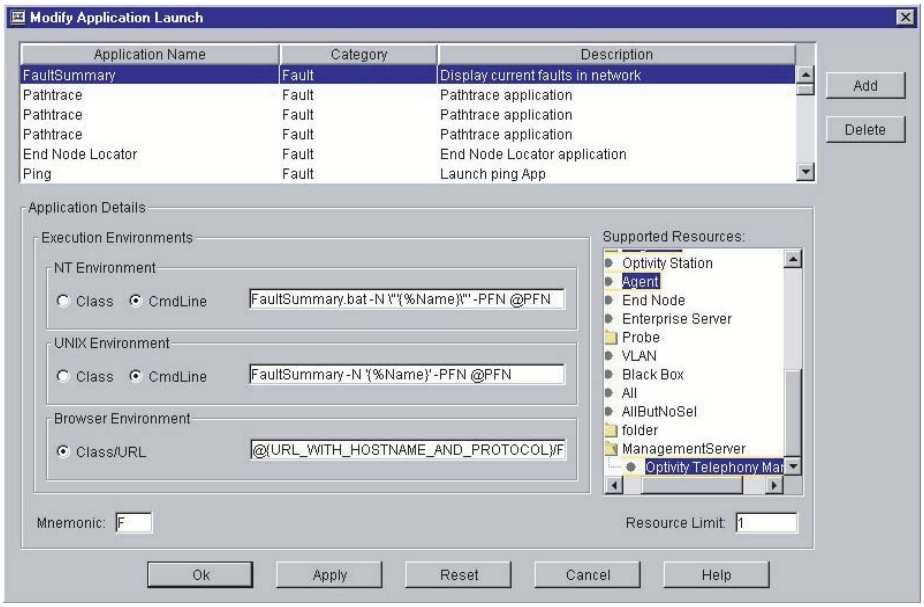
When Optivity NMS and OTM co-reside on the same server, the OTM Trap system disables its Trap server and instead interfaces with the Optivity Trap server to receive traps.

Upon receiving a system alarm (or other traps that it has been configured to handle), OTM reformats it and forwards it to Optivity NMS. Optivity NMS recognizes the trap (from OIT definitions) and should now be able to reflect the changed status.

Procedure 49
Setting up FaultSummary

1. Select Application Launch from InfoCenter’s top menu.
2. Select the Fault Summary application. See Figure 109 on page 228.
3. While holding down the Ctrl and Shift keys, select the Managementserver > Optivity Telephony Manager resource to enable FaultSummary for OTM.
4. Click **Apply**.

Figure 109
Modify Application Launch dialog box



Modify Application Launch

Application Name	Category	Description
FaultSummary	Fault	Display current faults in network
Pathtrace	Fault	Pathtrace application
Pathtrace	Fault	Pathtrace application
Pathtrace	Fault	Pathtrace application
End Node Locator	Fault	End Node Locator application
Ping	Fault	Launch ping App

Application Details

Execution Environments

NT Environment

○ Class ● CmdLine `FaultSummary.bat -N \"{%Name}\" -PFN @PFN`

UNIX Environment

○ Class ● CmdLine `FaultSummary -N '{%Name}' -PFN @PFN`

Browser Environment

● Class/URL `@{URL_WITH_HOSTNAME_AND_PROTOCOL}/F`

Supported Resources:

- Optivity Station
- Agent
- End Node
- Enterprise Server
- Probe
- VLAN
- Black Box
- All
- AllButNoSel
- folder
- ManagementServer
  - Optivity Telephony Mar

Mnemonic: F

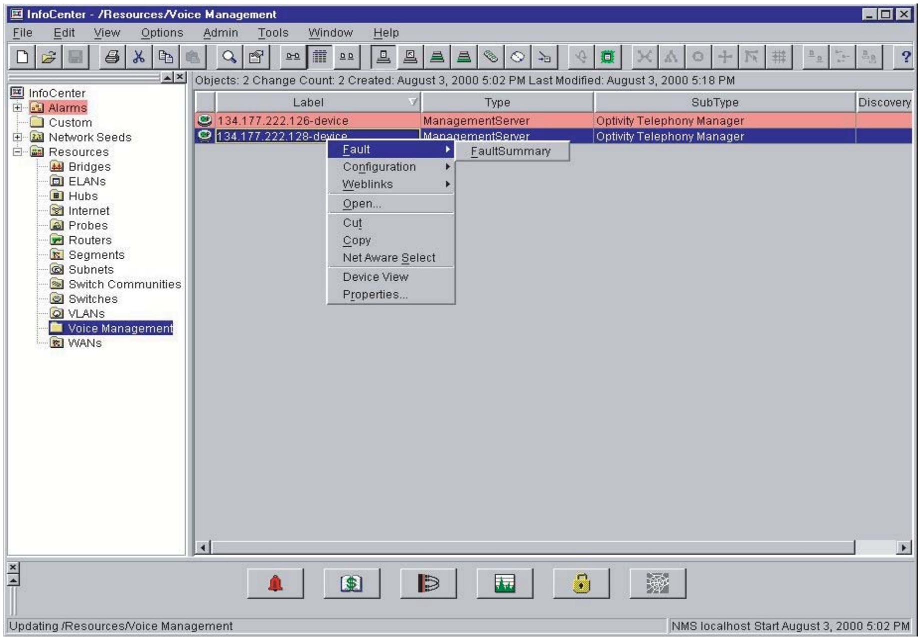
Resource Limit: 1

End of Procedure

Procedure 50
Launching FaultSummary

Select the OTM icon and use the right-click menu to launch FaultSummary. See Figure 110 on page 229.

Figure 110
Launch FaultSummary



InfoCenter - /Resources/Voice Management

Objects: 2 Change Count: 2 Created: August 3, 2000 5:02 PM Last Modified: August 3, 2000 5:18 PM

Label	Type	SubType	Discovery
134.177.222.126-device	ManagementServer	Optivity Telephony Manager	
134.177.222.128-device	ManagementServer	Optivity Telephony Manager	

Updating /Resources/Voice Management

NMS localhost Start August 3, 2000 5:02 PM

End of Procedure

Configuring OTM

CAUTION — Service Interruption

OTM is included in the device file to monitor the alarms received from the OTM server. When OTM co-resides with ONMS, the trap server is shared and both ONMS and OTM receive and process all traps. In this case, the number of traps is multiplied and the trap server receives a large volume of traps, which can cause the trap server to crash. To prevent this, you must modify the notification script on the co-resident OTM system so that traps are not forwarded to the OTM server.

The Optivity Telephony Manager server must be set up to forward traps to Optivity NMS. Forwarded traps must be in the OTM Open Alarm II format to be recognized.

The OTM Alarm notification application forwards traps of interest to Optivity NMS.

Sample scripts are provided with the Alarm Notification application, which you can modify in the following ways to forward traps:

- Change the target IP to the address of the Optivity NMS server.
- Select the severity of the traps that you want to forward: Critical, Major, Minor.
- Modify the sample scripts to forward traps to Optivity NMS.

  Note: Take care to translate the incoming trap to OTM Open Alarm II, and set the proper device identification and error code fields.

These traps, when received by Optivity NMS, result in a change of status of OTM and can be viewed through the Fault Summary.

Removing an OTM server

Procedure 51
Removing an OTM server

1 In InfoCenter, open a folder in the Folders pane.

2 Select the OTM server that you want to delete.

3 From the InfoCenter menu bar, choose **File > Delete**. This action deletes the object from Optivity NMS.

End of Procedure

Troubleshooting

If you do not see the OITHOME environment variable, you must manually set it before installing OTM or manually running oitInstall to update the Optivity NMS database.

If you do not see Managementserver type and Optivity Telephony Manager sub-type on the Device — Add panel:

- Check to see if the OITHOME variable was set.
- Check to see if the OTM OIT files are present and in the correct folder.
- Check the oitInstall log file to verify that the OTM entries were updated.
- You may need to run oitInstall again.

If you cannot see the OTM server that you have added:

- Check the View Properties of the folder to verify that it can display OTM servers.

If you cannot launch or connect to OTM web applications:

- Verify that the IP Address of the OTM server entered in InfoCenter is correct.
- Verify that the OTM web server is running.
- Verify that you have the proper Java Plug-In installed.

If you are not receiving traps from an OTM server:

- Verify that the OTM Alarm Notification application is running and receiving traps.
- Verify that the OTM Alarm Notification scripts are configured to send traps to Optivity NMS.
- Check the oitInstall log files to verify that the OTM entries were updated.
- Check the status of Optivity NMS daemons from Control Panel > Services, or by typing **`optstatus -fe`** at the command prompt.

If you cannot launch Fault Summary for OTM:

- Check the Application Launch entries. FaultSummary should be enabled for Managementserver > Optivity Telephony Manager.

Integrating OTM with HP OpenView

Contents

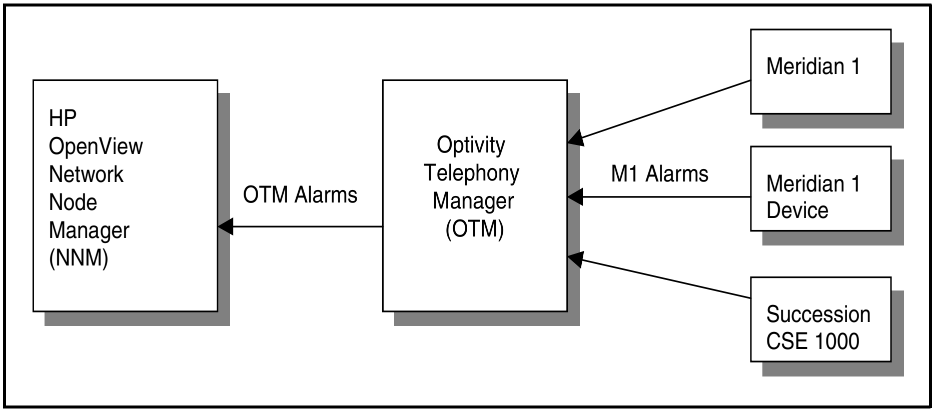
This chapter contains information on the following topics:

Overview

This chapter provides information on the integration of the HP* OpenView* (HP OV) Network Node Manager (NNM) management platform with Nortel's Optivity Telephony Manager (OTM). It discusses the type of integration supported. The included procedures provide detailed step-by-step instructions on how to configure HP OV NNM to access OTM-related functionality and information.

Nortel's technical support for this feature is limited to support of the two software files that are distributed with OTM, *OtmOpenAlarms.mib* and *OtmStMon.exe*. These files are compatible with the version of HP OpenView that was current at the time your OTM software was released.

Figure 111
OTM alarm integration with HP OpenView Network Node Manager


HP OpenView Network Node Manager (NNM)
OTM Alarms
Optivity Telephony Manager (OTM)
M1 Alarms
Meridian 1
Meridian 1 Device
Succession CSE 1000

As seen in Figure 111, CS 1000 and Meridian 1 systems, Meridian Mail, and other devices send their alarms to the OTM server, which can then collect the alarms and forward them to the NNM. The NNM appears the OTM alarms in its Alarm Browser and updates the color of the OTM object in the Network Map to reflect the current status of the OTM server, or the status of the devices the OTM server manages. In addition, you can also configure the NNM to allow the network administrator easy access to the OTM server.

Refer to *Optivity Telephony Manager: System Administration* (553-3001-330) for information on configuring the OTM server to forward alarms to an external management station.

Limitations

- Coresidency is not supported for NNM and OTM on the same PC. However, for web clients, if JRE 1.4.2 is loaded in the system and the default web browser is Internet Explorer, both OTM and HP OpenView web applications can be launched simultaneously.
- The OTM server does not support auto-discovery from NNM.

Hardware and software requirements

PC hardware requirements (HP OV PC)

Refer to HP OV NNM documentation for details.

PC software requirements (HP OV PC)

- HP OV NNM Release 6.*x*
- OTM Alarm Integration Package:
  - OTM Alarm MIB (OtmOpenAlarms.mib)
  - OTM Status Monitor (OtmStMon.exe)

OTM software requirements (OTM PC)

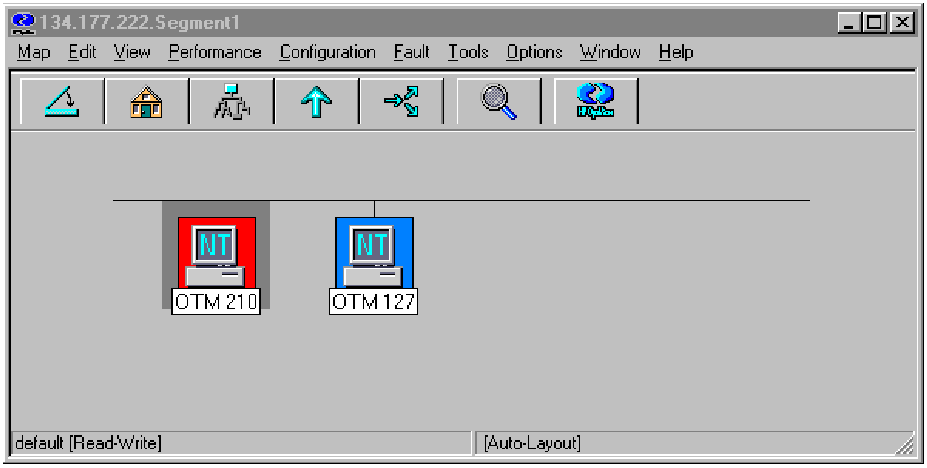
- OTM Release 1.01 or later with:
  - Alarm Notification application
  - web-based alarm browser

System integration

HP OV NNM Network Map

On the NNM Network Map. See Figure 112 on page 236, an OTM server can be represented as an object. You can configure incoming events to trigger a color change to the object icon to indicate the current status of the OTM server or of the devices monitored by the OTM server.

Figure 112
HP OpenView Network Node Manager Network Map

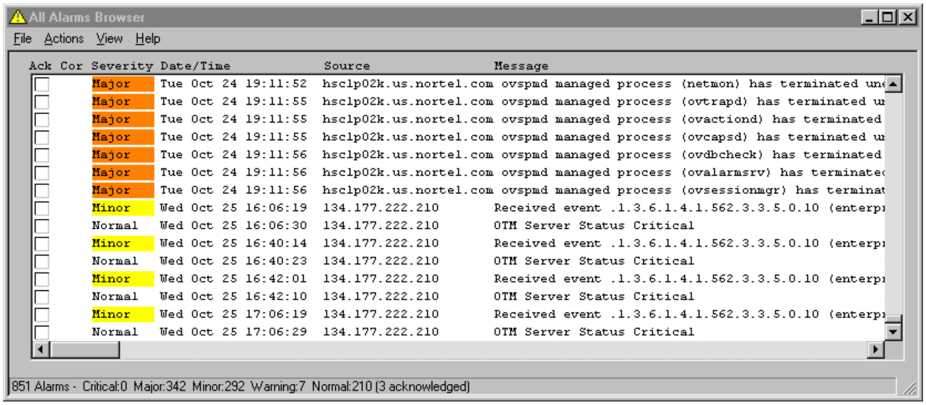


The OTM Status Monitor (OtmStMon) is the program that is used to update the color of the icon for an OTM object. When the color is changed upon the receipt of an incoming event, a message is also logged and appears in the NNM Alarm Browser to indicate the status update.

HP OV NNM Alarm Browser

You can display contents of incoming OTM events in the NNM Alarms Browser. See Figure 113.

Figure 113
HP OV NNM Alarms Browser

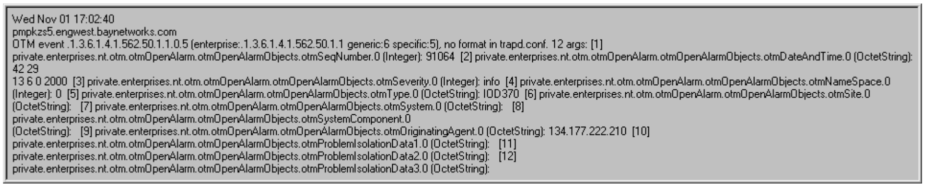


Ack	Cor	Severity	Date/Time	Source	Message
□		Major	Tue Oct 24 19:11:52	hsclp02k.us.nortel.com	ovspmd managed process (netmon) has terminated un
□		Major	Tue Oct 24 19:11:55	hsclp02k.us.nortel.com	ovspmd managed process (ovtrapd) has terminated u
□		Major	Tue Oct 24 19:11:55	hsclp02k.us.nortel.com	ovspmd managed process (ovactiond) has terminated
□		Major	Tue Oct 24 19:11:55	hsclp02k.us.nortel.com	ovspmd managed process (ovcapsd) has terminated u
□		Major	Tue Oct 24 19:11:56	hsclp02k.us.nortel.com	ovspmd managed process (ovdbcheck) has terminated
□		Major	Tue Oct 24 19:11:56	hsclp02k.us.nortel.com	ovspmd managed process (ovalarmsrv) has terminate
□		Major	Tue Oct 24 19:11:56	hsclp02k.us.nortel.com	ovspmd managed process (ovsessionmgr) has terminat
□		Minor	Wed Oct 25 16:06:19	134.177.222.210	Received event .1.3.6.1.4.1.562.3.3.5.0.10 (enterp
□		Normal	Wed Oct 25 16:06:30	134.177.222.210	OTM Server Status Critical
□		Minor	Wed Oct 25 16:40:14	134.177.222.210	Received event .1.3.6.1.4.1.562.3.3.5.0.10 (enterp
□		Normal	Wed Oct 25 16:40:23	134.177.222.210	OTM Server Status Critical
□		Minor	Wed Oct 25 16:42:01	134.177.222.210	Received event .1.3.6.1.4.1.562.3.3.5.0.10 (enterp
□		Normal	Wed Oct 25 16:42:10	134.177.222.210	OTM Server Status Critical
□		Minor	Wed Oct 25 17:06:19	134.177.222.210	Received event .1.3.6.1.4.1.562.3.3.5.0.10 (enterp
□		Normal	Wed Oct 25 17:06:29	134.177.222.210	OTM Server Status Critical

851 Alarms - Critical:0 Major:342 Minor:292 Warning:7 Normal:210 (3 acknowledged)

You can also highlight a specific alarm message on the NNM Alarms Browser, and right-click to display the message content in a separate window. See Figure 114. You can then analyze the different variables and their values.

Figure 114
Alarm message content



```
Wed Nov 01 17:02:40
pmpkzs5.engwest.baynetworks.com
OTM event .1.3.6.1.4.1.562.50.1.1.0.5 (enterprise:.1.3.6.1.4.1.562.50.1.1 generic:6 specific:5), no format in trapd.conf. 12 args: [1]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSeqNumber.0 (Integer): 91064  [2] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmDateAndTime.0 (OctetString):
42 29
13 6 0 2000  [3] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSeverity.0 (Integer): info  [4] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmNameSpace.0
(Integer): 0  [5] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmType.0 (OctetString): IOD370  [6] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSite.0
(OctetString):   [7] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSystem.0 (OctetString):   [8]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSystemComponent.0
(OctetString):   [9] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmOriginatingAgent.0 (OctetString): 134.177.222.210  [10]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmProblemIsolationData1.0 (OctetString):   [11]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmProblemIsolationData2.0 (OctetString):   [12]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmProblemIsolationData3.0 (OctetString):
```

OTM web Access

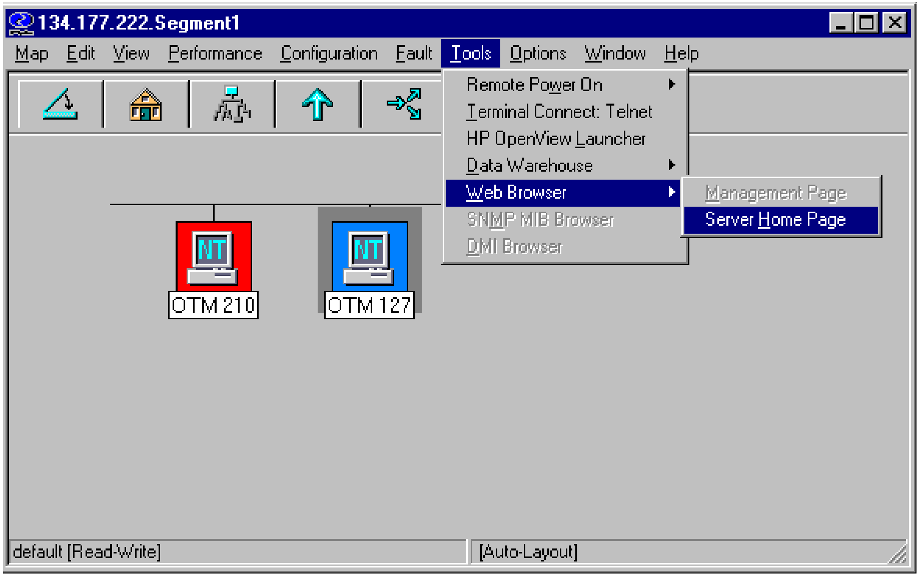
Procedure 52
Accessing OTM

To access the OTM server from NNM:

1 Highlight the OTM object on the Network.

2 Select Tools > web Browser > server Home Page Figure 115 on page 238.

Figure 115
OTM web Access



Your default web browser is brought up with the web-based OTM interface. You can log in to the OTM web and access the various OTM applications including the OTM Alarm Browser.

End of Procedure

Installation and configuration

OTM Alarm Integration Package (HP OV PC)

1 Copy the OtmStMon.exe to the Openview/bin ($OV_BIN) directory.

2 Copy the OtmOpenAlarms.mib to the directory $OV_SNMP_MIB/Vendor/Nortel. Create this directory if it does not already exist.

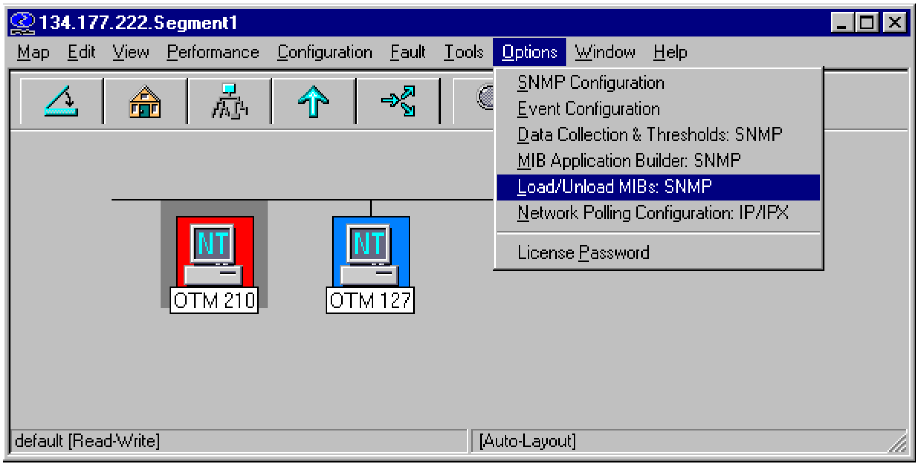
HP OV NNM (HP OV PC)

The following configuration procedures are performed while NNM is running:

Procedure 53
Installing OTM Alarm MIB

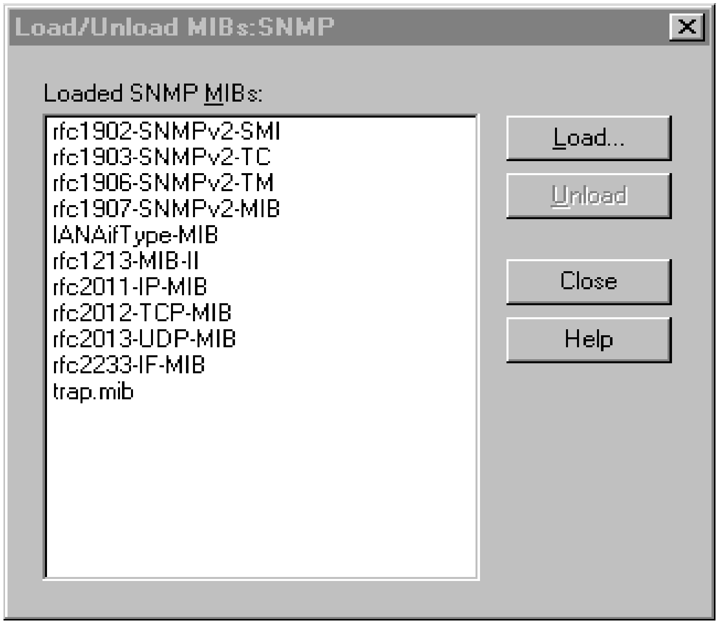
1 Select **Options > Load/Unload MIBs: SNMP**. See Figure 116.

Figure 116
NNM Load/Unload MIBs



2 Click **Load** in the Load/Unload MIBs dialog box. See Figure 117 on page 240.

Figure 117
Load/Unload MIBs

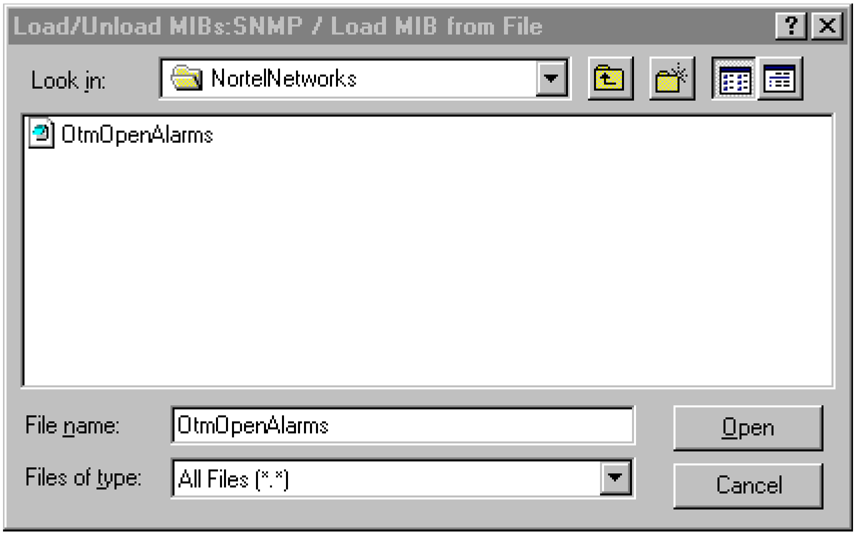


Loaded SNMP MIBs:

rfc1902-SNMPv2-SMI
rfc1903-SNMPv2-TC
rfc1906-SNMPv2-TM
rfc1907-SNMPv2-MIB
IANAifType-MIB
rfc1213-MIB-II
rfc2011-IP-MIB
rfc2012-TCP-MIB
rfc2013-UDP-MIB
rfc2233-IF-MIB
trap.mib

3 Open the OtmOpenAlarms.mib file. See Figure 118.

Figure 118
Load MIB



Look in: NortelNetworks

File name: OtmOpenAlarms

Files of type: All Files (*.*)

The OTM alarm MIB definitions are now loaded into the NNM's MIB database.

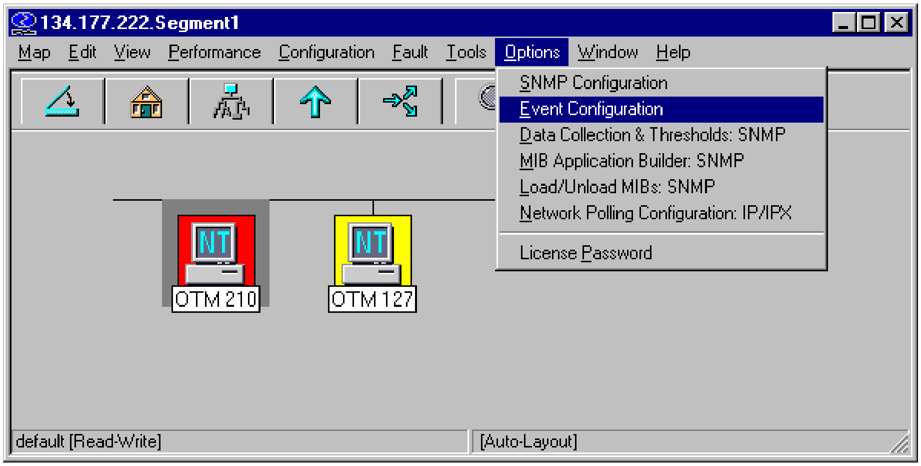
End of Procedure

Procedure 54
Configuring an event

After the OTM Alarm MIB is loaded, actions must be defined through the NNM Event Configuration for each OTM event.

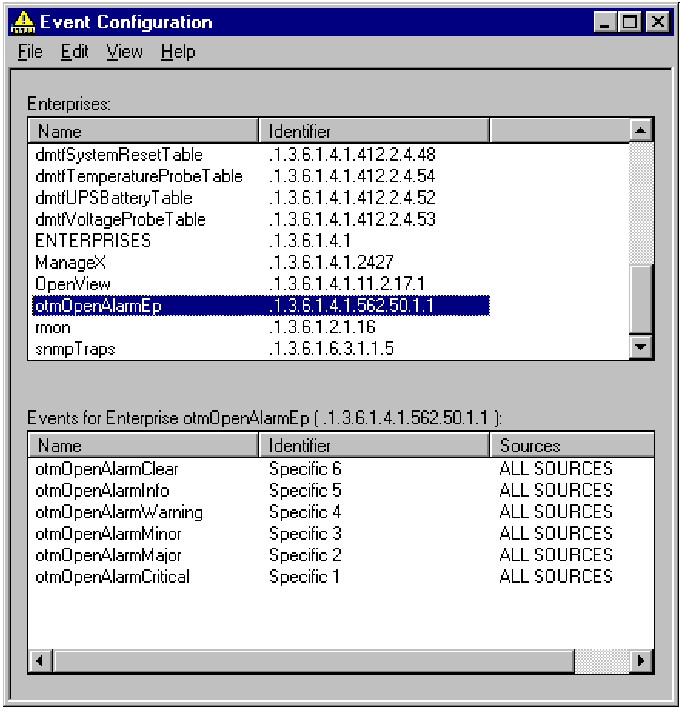
1 Select **Options > Event Configuration**. See Figure 119.

Figure 119
NNM Main Menu - Event Configuration



2 Locate and select "otmOpenAlarmEp" from the list of Enterprises. See Figure 120 on page 242.

Figure 120
Event Configuration



Enterprises:

Name	Identifier
dmtfSystemResetTable	.1.3.6.1.4.1.412.2.4.48
dmtfTemperatureProbeTable	.1.3.6.1.4.1.412.2.4.54
dmtfUPSBatteryTable	.1.3.6.1.4.1.412.2.4.52
dmtfVoltageProbeTable	.1.3.6.1.4.1.412.2.4.53
ENTERPRISES	.1.3.6.1.4.1
ManageX	.1.3.6.1.4.1.2427
OpenView	.1.3.6.1.4.1.11.2.17.1
otmOpenAlarmEp	.1.3.6.1.4.1.562.50.1.1
rmon	.1.3.6.1.2.1.16
snmpTraps	.1.3.6.1.6.3.1.1.5

Events for Enterprise otmOpenAlarmEp (.1.3.6.1.4.1.562.50.1.1):

Name	Identifier	Sources
otmOpenAlarmClear	Specific 6	ALL SOURCES
otmOpenAlarmInfo	Specific 5	ALL SOURCES
otmOpenAlarmWarning	Specific 4	ALL SOURCES
otmOpenAlarmMinor	Specific 3	ALL SOURCES
otmOpenAlarmMajor	Specific 2	ALL SOURCES
otmOpenAlarmCritical	Specific 1	ALL SOURCES

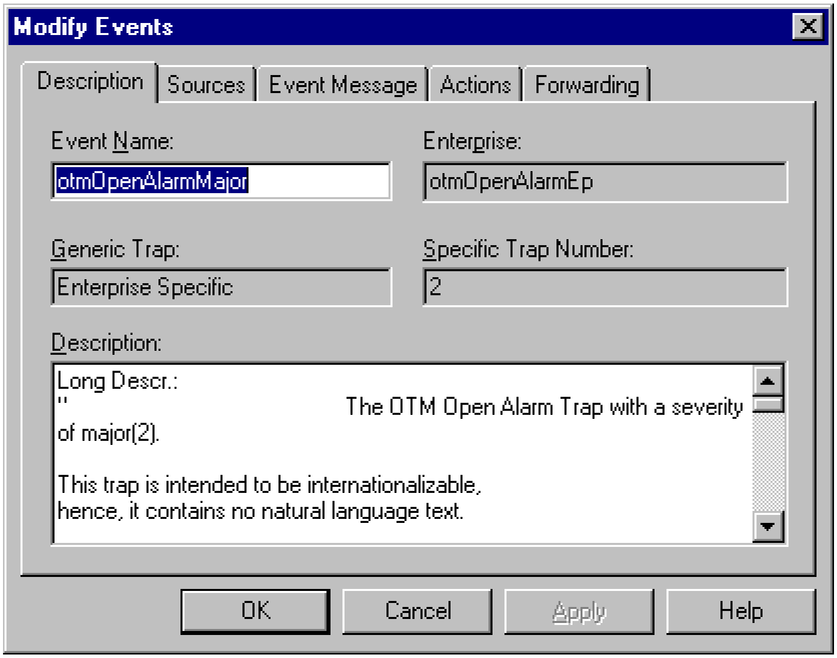
There are six events defined for the otmOpenAlarmEp Enterprise. For each event, you configure the desired actions to be taken if the event occurs.

Use the OTM Major Alarm event (otmOpenAlarmMajor, Specific 2) as an example:

3 Double-click the corresponding entry on the list.

The Modify Events dialog box appears. See Figure 121 on page 243.

Figure 121
Modify Events - Description



Event Name: otmOpenAlarmMajor

Enterprise: otmOpenAlarmEp

Generic Trap: Enterprise Specific

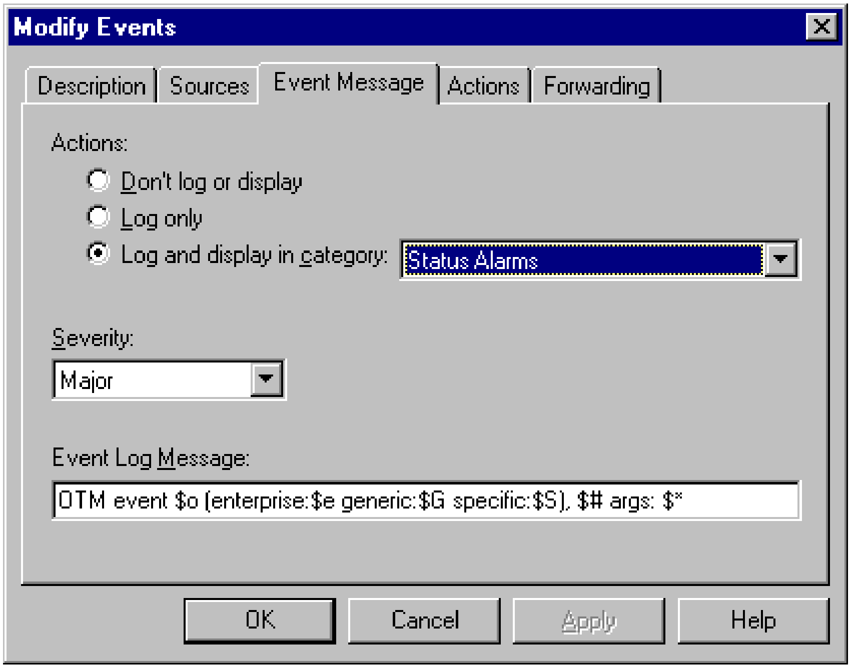
Specific Trap Number: 2

Description:

```
Long Descr.:
"                                   The OTM Open Alarm Trap with a severity
of major(2).

This trap is intended to be internationalizable,
hence, it contains no natural language text.
```

4 Select the Event Message tab. See Figure 122 on page 244.

Figure 122
Modify Events - Event Message



Actions:

○ Don't log or display

○ Log only

● Log and display in category: Status Alarms

Severity: Major

Event Log Message: OTM event $o (enterprise:$e generic:$G specific:$S), $# args: $*

5 Configure the following:

a. Actions: Select Log and display in category: Status Alarms.

This enables the display of the incoming event message in the NNM Alarm Browser.

b. Severity: Select Major for this event.

c. Event Log Message: Enter the following default text:

OTM event $o (enterprise:$e generic:$G specific:$S), $# args: $*

The displayed message shows the contents of the event message. See Table 12 on page 245 for other variables.

You are allowed to display any message that you choose in the Alarm Browser.

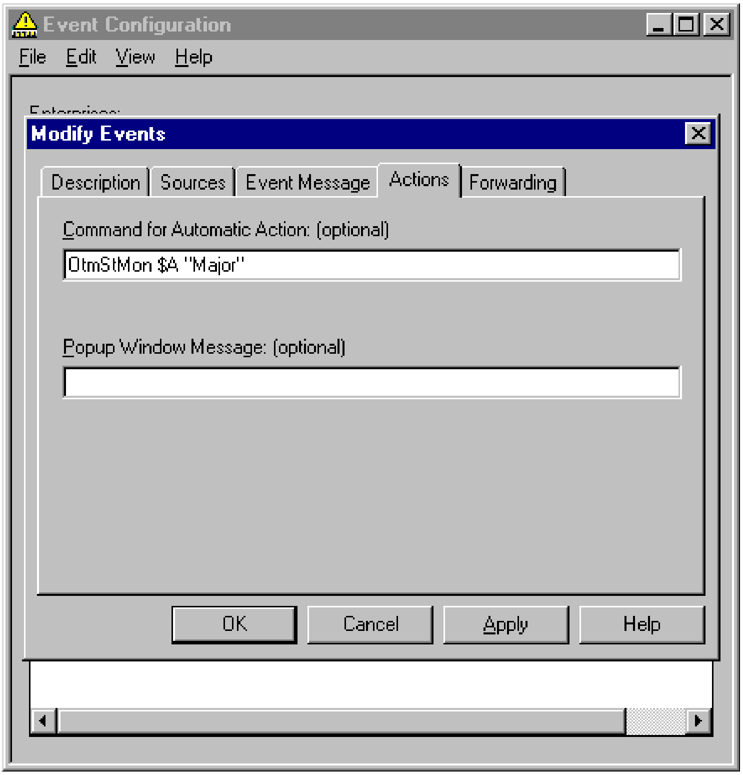
End of Procedure

Table 12
Legend for $ variables in the Event Log Message

Variable	Action
$o	Print the name (object identifier) of the received event as a string of numbers.
$e	Print the trap enterprise as an Object ID string of numbers. This number is implied by the event object identifier for non-SNMPv1 events.
$G	Print the trap's generic-trap number. This number is implied by the event object identifier for non-SNMPv1 events.
$S	Print the trap's specific-trap number. This number is implied by the event object identifier for non-SNMPv1 events.
$#	Print the number of attributes in the event.
$*	Print all the attributes as *seq* name (type): value strings, where *seq* is the attribute sequence number.

If you also want the color of the object on the map to change to reflect the occurrence of the incoming event, you can also invoke the OTM Status Monitor (OtmStMon.exe) by specifying a call to it under the "Actions" item. See Figure 123 on page 246.

Figure 123
Modify Events - Actions



Command for Automatic Action: (optional)

OtmStMon $A "Major"

Popup Window Message: (optional)

OTM Status Monitor

The OTM Status Monitor enables you to change the color of the OTM object on the Network Map to reflect the current status of the server. In addition, a message is also logged onto the HP OV NNM Alarm Browser to indicate the status change.

OtmStMon is written in C and makes use of the HP OV ovevent application. OtmStMon takes in two parameters: an object's selection name and a textual representation of the new status (for example, Critical or Normal). If ovevent cannot locate an object on the current Network Map with the specified selection name, an error message appears. Therefore, if an OTM object is not defined in the Network Map, OtmStMon should not be invoked for an event.

The invocation format for OtmStMon is as follows:

OtmStMon <*selection_name*> <*object_status*>

where

<*selection_name*> is HP OV NNM’s unique selection name for an object item on the Network Map.

<*object_status*> is one of the following textual strings: Unknown, Normal, Warning, Minor, Major, Critical, Restricted, Testing, Disabled, Managed, Unmanaged.

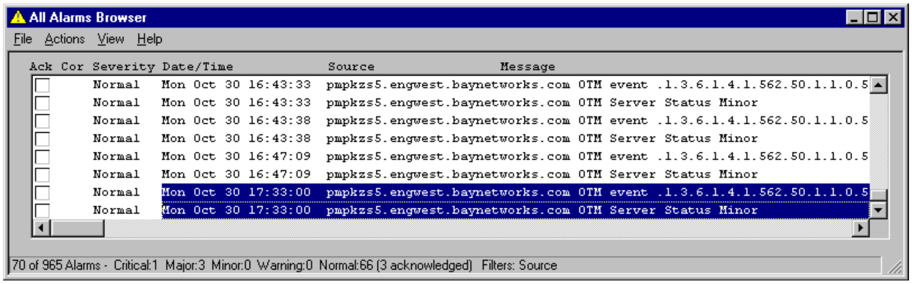
If the OTM Status Monitor is not called, then the color of the object that appears on the Network Map does not change for the incoming event.

If no object is defined for the OTM server on the Network Map, a call to OTM Status Monitor results in an error. Therefore, do not specify calls to OtmStMon if there is no OTM server defined on the Map.

A call to the OTM Status Monitor results in a message, in addition to the original incoming event message, appearing in the NNM All Alarms Browser. See Figure 124. This message is logged whenever the OTM Status Monitor changes the color of an object.

Not every incoming OTM event necessitates the changing of the object’s color. For example, a minor or info event may not need to alert the customer. In these cases, the customer may want to configure these events in such a way to simply log the incoming event message and not call OtmStMon.

Figure 124
All Alarms Browser



```
Ack Cor Severity Date/Time            Source                          Message
□          Normal   Mon Oct 30 16:43:33  pmpkzs5.engwest.baynetworks.com OTM event .1.3.6.1.4.1.562.50.1.1.0.5
□          Normal   Mon Oct 30 16:43:33  pmpkzs5.engwest.baynetworks.com OTM Server Status Minor
□          Normal   Mon Oct 30 16:43:38  pmpkzs5.engwest.baynetworks.com OTM event .1.3.6.1.4.1.562.50.1.1.0.5
□          Normal   Mon Oct 30 16:43:38  pmpkzs5.engwest.baynetworks.com OTM Server Status Minor
□          Normal   Mon Oct 30 16:47:09  pmpkzs5.engwest.baynetworks.com OTM event .1.3.6.1.4.1.562.50.1.1.0.5
□          Normal   Mon Oct 30 16:47:09  pmpkzs5.engwest.baynetworks.com OTM Server Status Minor
□          Normal   Mon Oct 30 17:33:00  pmpkzs5.engwest.baynetworks.com OTM event .1.3.6.1.4.1.562.50.1.1.0.5
□          Normal   Mon Oct 30 17:33:00  pmpkzs5.engwest.baynetworks.com OTM Server Status Minor

70 of 965 Alarms -  Critical:1  Major:3  Minor:0  Warning:0  Normal:66 (3 acknowledged)  Filters: Source
```

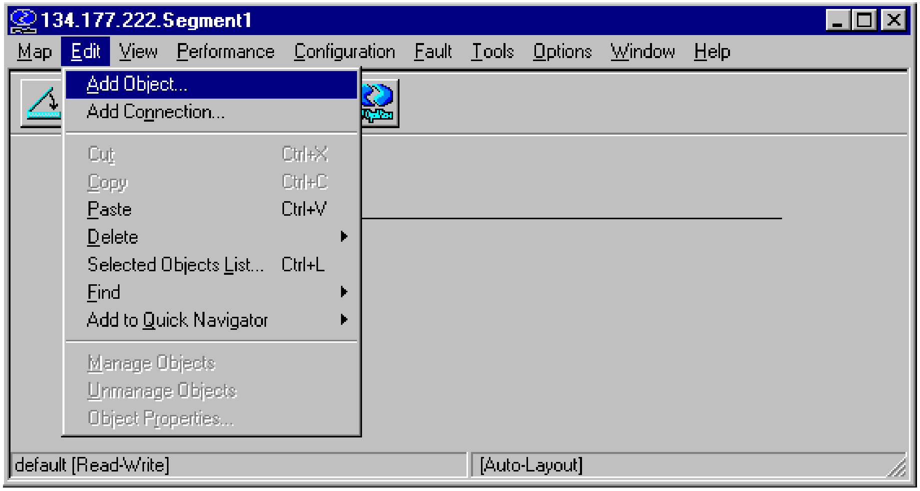
Procedure 55
Setting up a Network Map

To set up an OTM server object on the Network Map:

1 Locate the appropriate place in the Network Map for the OTM server.

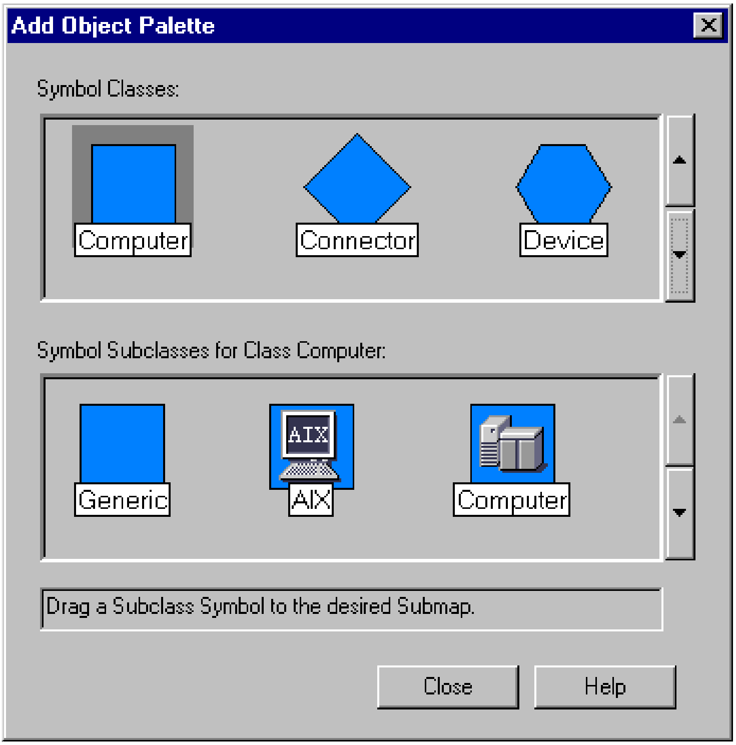
2 Select **Edit > Add Object**. See Figure 125 on page 248.

Figure 125
NNM Edit - Add Object



3 Select **Computer** from the Symbol Classes in the **Add Object Palette** dialog box. See Figure 126 on page 249.

Figure 126
Add Object Palette dialog box

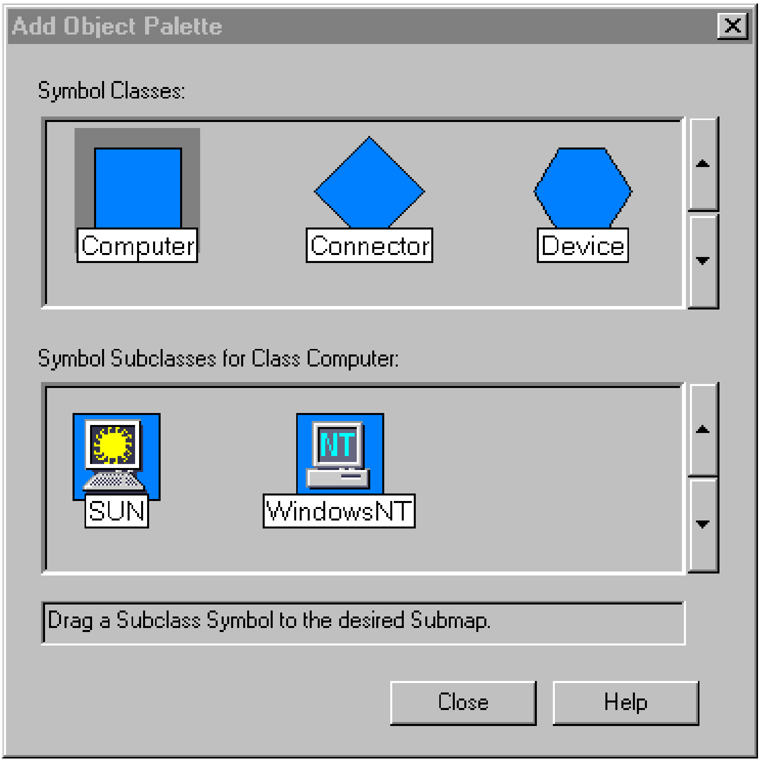


Drag a Subclass Symbol to the desired Submap.

4 Select and drag the standard WindowsNT icon from the Symbol Subclasses. See Figure 127 on page 250 onto the appropriate location on the Network Map.

The Add Object dialog box opens.

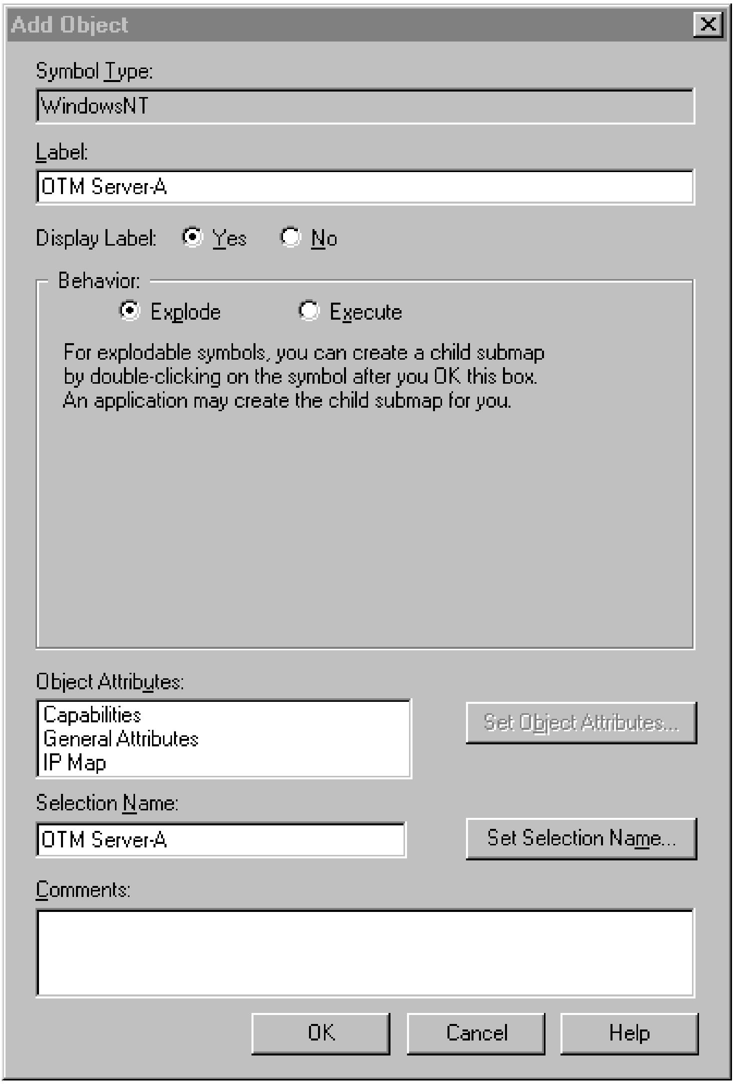
Figure 127
Add Object Palette dialog box II



Drag a Subclass Symbol to the desired Submap.

5 Fill in the Label field (OTM server-A in this example). See Figure 128 on page 251.

Figure 128
Add Object dialog box



Add Object

Symbol Type: WindowsNT

Label: OTM Server-A

Display Label: ● Yes ○ No

Behavior: ● Explode ○ Execute

For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.

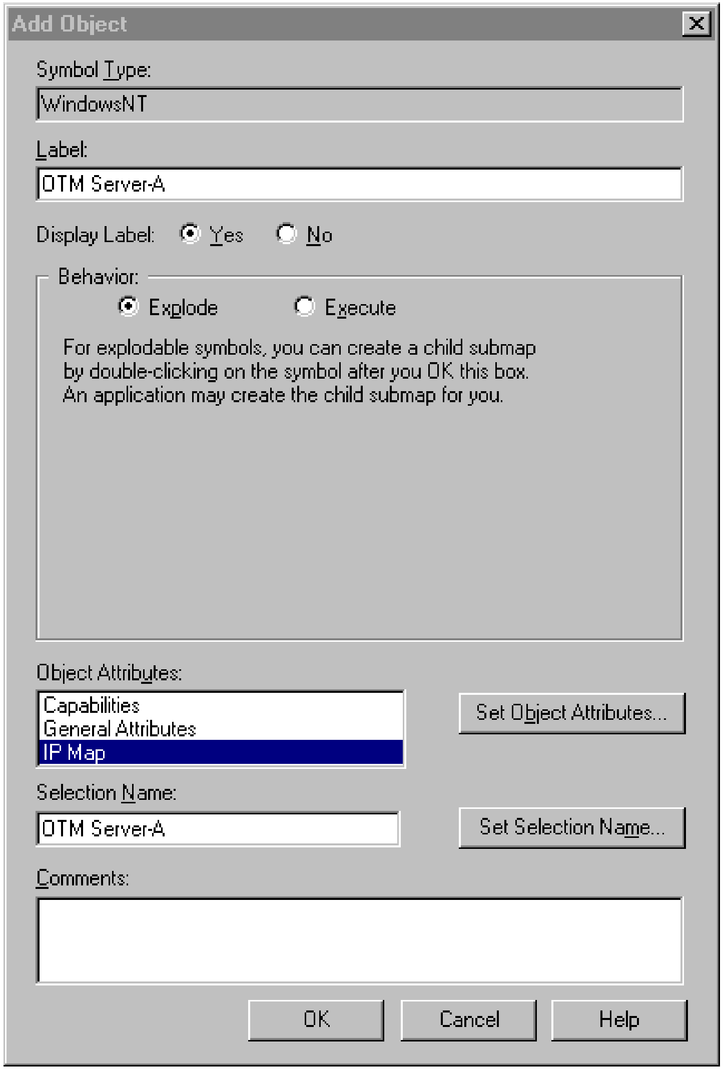
Object Attributes:
Capabilities
General Attributes
IP Map

Selection Name: OTM Server-A

Comments:

6 Select **IP Map** under Object Attributes, and click **Set Object Attributes.** See Figure 129 on page 252.

Figure 129
Add Object - IP Map



Add Object

Symbol Type: WindowsNT

Label: OTM Server-A

Display Label: ● Yes ○ No

Behavior: ● Explode ○ Execute

For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.

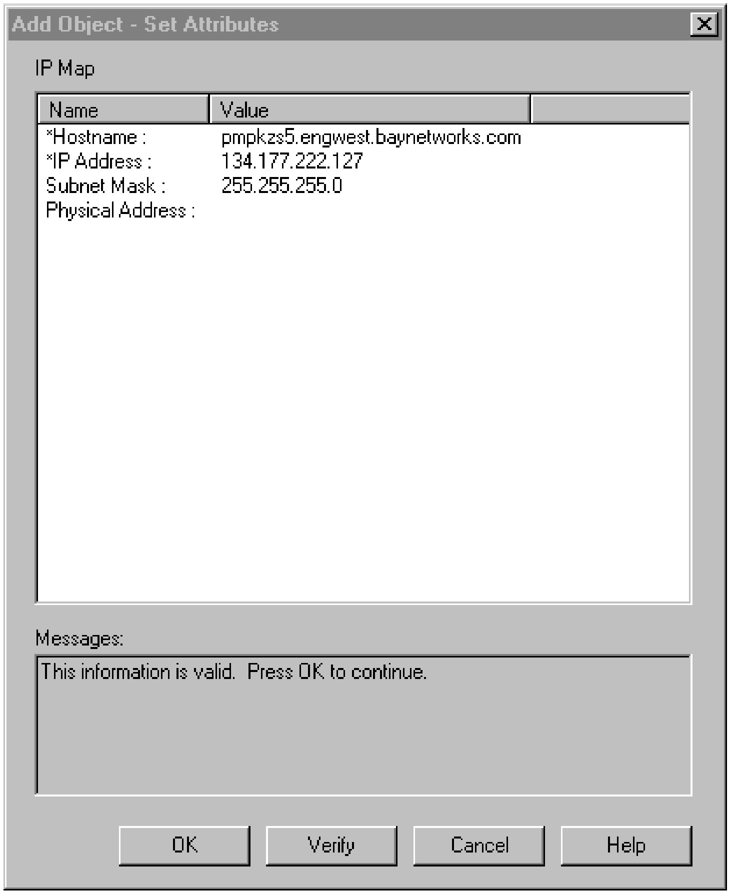
Object Attributes:
Capabilities
General Attributes
IP Map

Selection Name: OTM Server-A

Comments:

7 Select and enter the Hostname, IP Address, and Subnet Mask. See Figure 130 on page 253.

Figure 130
Add Object - Set Attributes dialog box



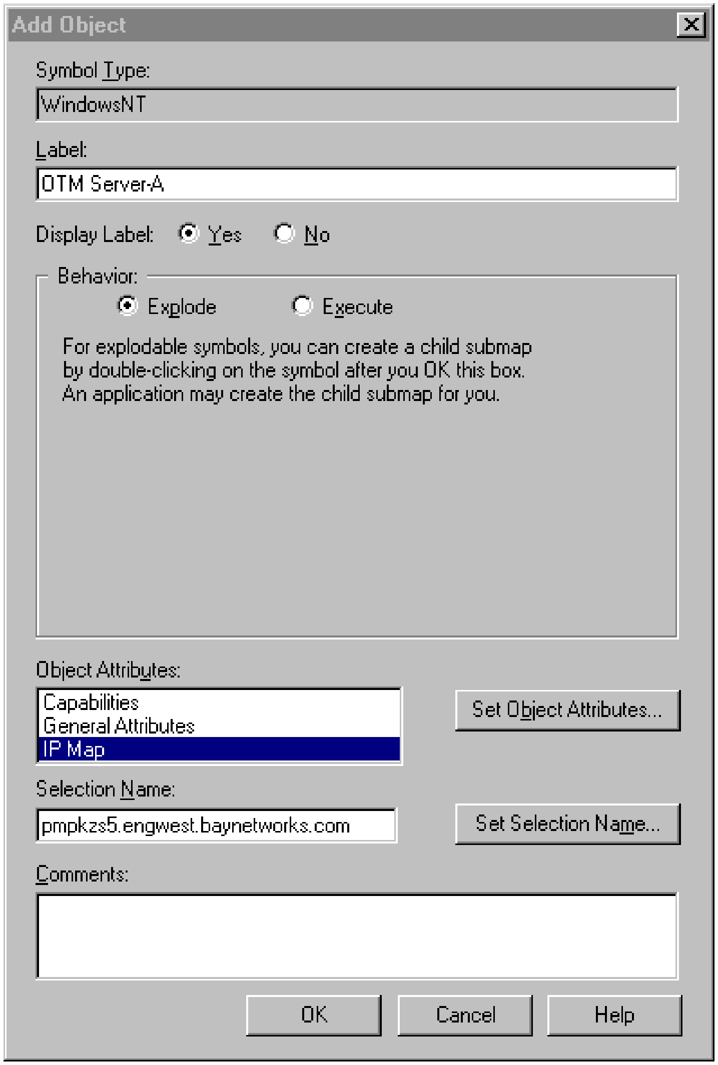
Name	Value
*Hostname :	pmpkzs5.engwest.baynetworks.com
*IP Address :	134.177.222.127
Subnet Mask :	255.255.255.0
Physical Address :	

Messages:

This information is valid. Press OK to continue.

8 Click **OK**. You are returned to the Add Object dialog box. In the Selection Name field, enter the same value as that of the Hostname in the previous step (pmpkzs5.engwest.baynetworks.com in this example). See Figure 131 on page 254.

Figure 131
Add Object - Selection Name



Symbol Type: WindowsNT

Label: OTM Server-A

Display Label: ● Yes ○ No

Behavior: ● Explode ○ Execute

For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.

Object Attributes:
Capabilities
General Attributes
IP Map

Selection Name: pmpkzs5.engwest.baynetworks.com

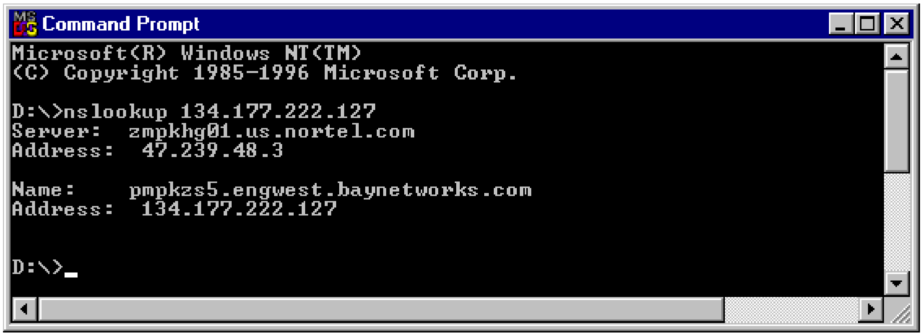
Comments:

9 Click **OK**. The object is created on the Network Map.

CAUTION — Service Interruption

The value for Hostname must be the domain name server (DNS) representation of the IP address (if the IP address can be resolved locally). Use the command **`nslookup`** to retrieve the DNS representation if you do not already know it. See Figure 132. If the IP address cannot be interpreted locally, then enter the dotted decimal representation.

Figure 132
nslookup command



```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

D:\>nslookup 134.177.222.127
Server:  zmpkhg01.us.nortel.com
Address:  47.239.48.3

Name:    pmpkzs5.engwest.baynetworks.com
Address:  134.177.222.127


D:\>_
```

10 If you want to indicate the status of the OTM server through the color of the object on the map, be sure to set the Status Source under Symbol Properties to Object. See Figure 133 on page 256 and Figure 134 on page 257).

Figure 133
NNM Main Menu - Symbol Properties

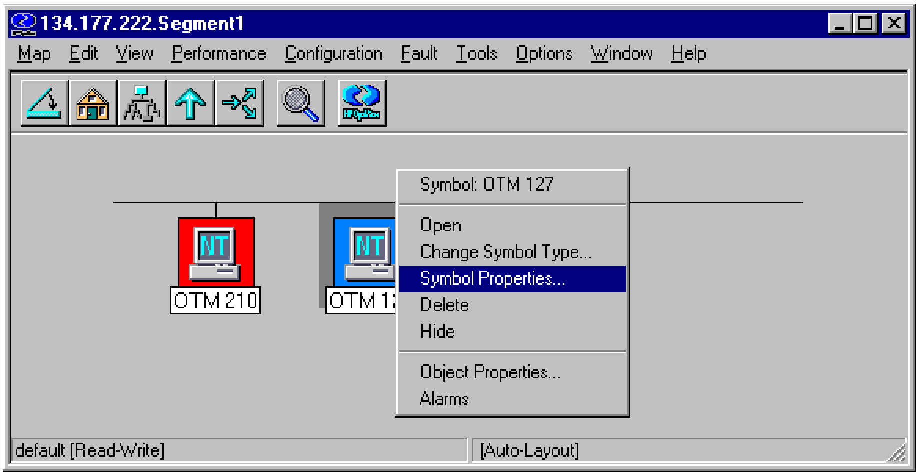
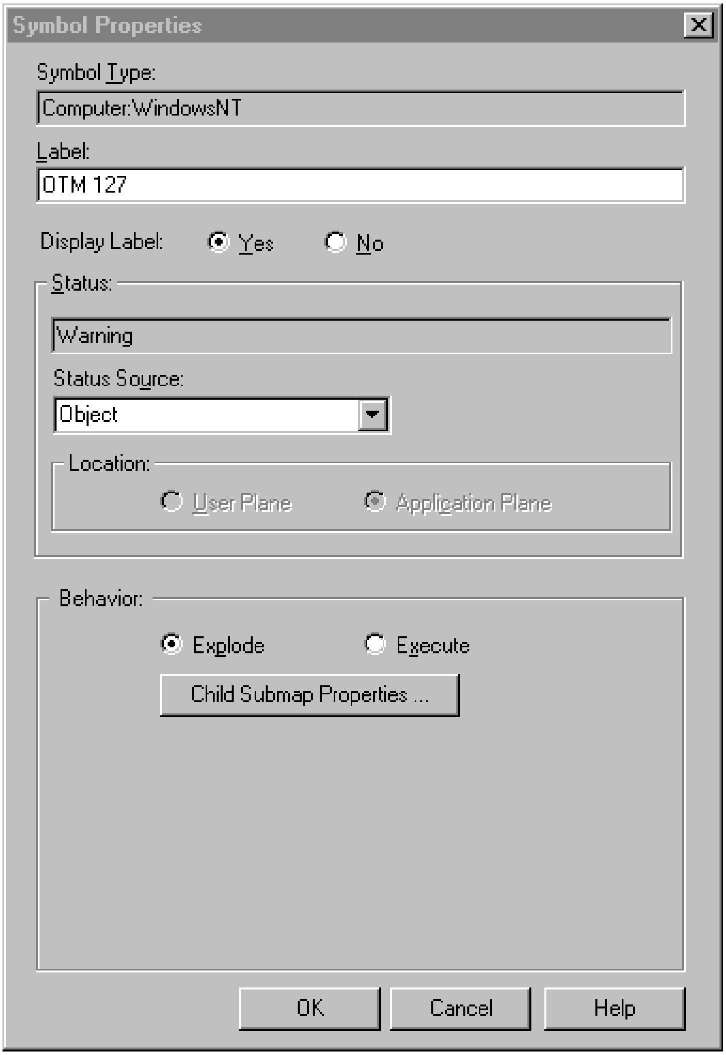


Figure 134
Symbol Properties dialog box



End of Procedure

Procedure 56
Configuring OTM web server Access

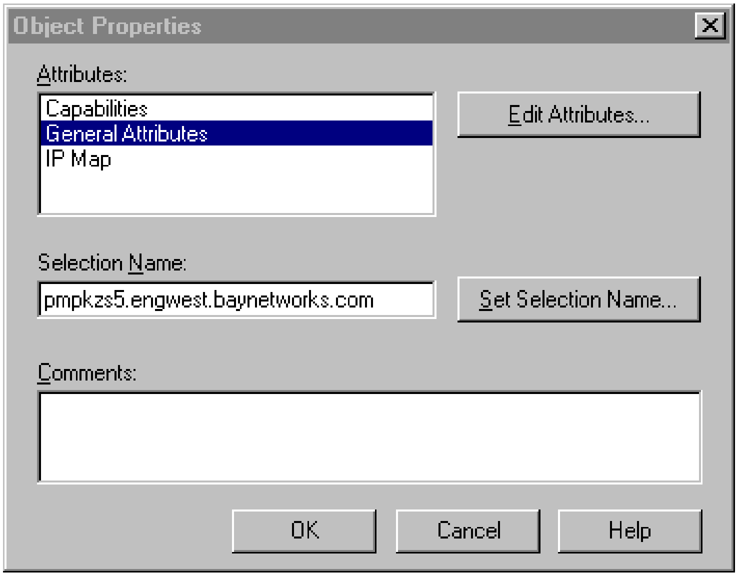
You can also configure the Management URL to access the OTM server. See Figure 135 on page 258 and Figure 136 on page 259.

For an object on the Network Map, under General Attributes in the Object Properties dialog box:

1 Enter the address (IP address or the DNS name) of the OTM server in the ManagementURL field.

2 Set isHTTPSupported to **True**.

Figure 135
Object Properties dialog box

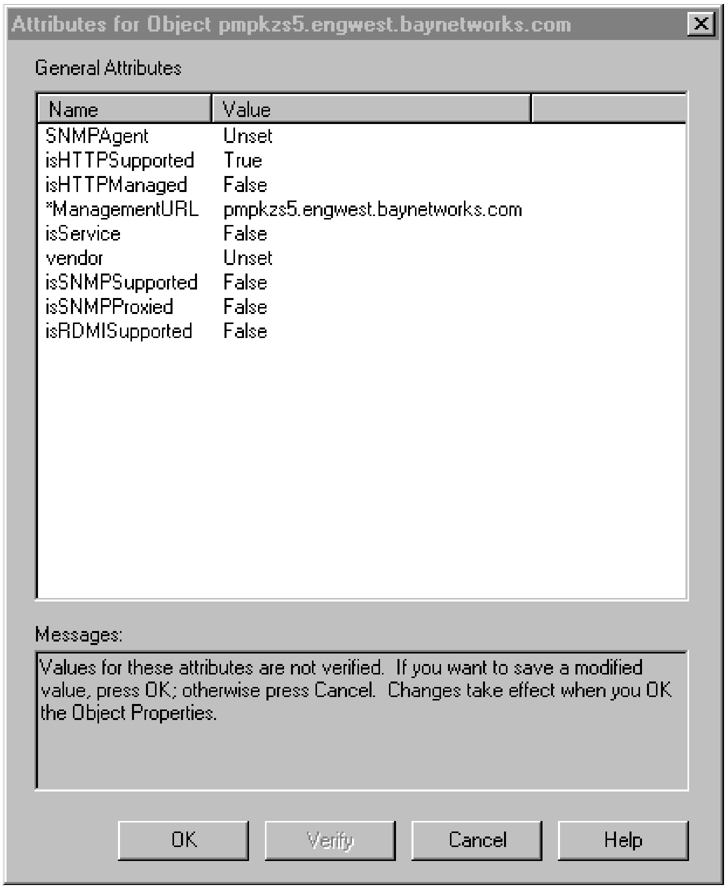


Attributes: General Attributes

Selection Name: pmpkzs5.engwest.baynetworks.com

Comments:

Figure 136
Attributes for Object dialog box



Attributes for Object pmpkzs5.engwest.baynetworks.com

General Attributes

Name	Value
SNMPAgent	Unset
isHTTPSupported	True
isHTTPManaged	False
*ManagementURL	pmpkzs5.engwest.baynetworks.com
isService	False
vendor	Unset
isSNMPSupported	False
isSNMPProxied	False
isRDMISupported	False

Messages:

Values for these attributes are not verified. If you want to save a modified value, press OK; otherwise press Cancel. Changes take effect when you OK the Object Properties.

End of Procedure

OTM configuration (OTM PC)

Refer to the Alarm Management section in *Optivity Telephony Manager: System Administration* (553-3001-330) for information on configuring the OTM server to forward SNMP traps to HP OV NNM or other remote systems.

Uninstalling OTM

Contents

This chapter contains information on the following topics:

Overview

This chapter contains information about using Uninstall to remove software that is no longer needed, or that has become damaged or was incorrectly installed.

Uninstalling OTM

Procedure 57
Uninstalling OTM

1 Access Uninstall

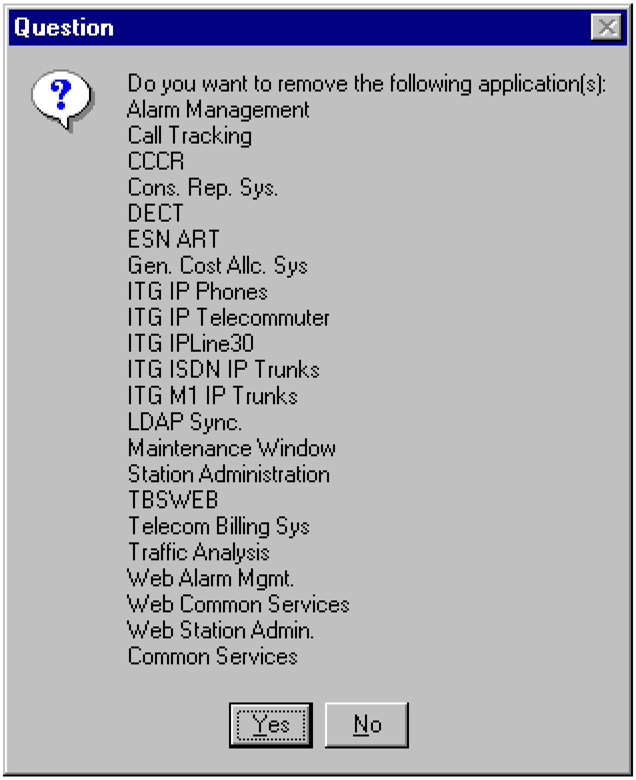
a. From the Start menu, select **Programs > Optivity Telephony Manager > OTM Uninstaller**.

or

b. In the Software Installation Wizard, select **Uninstall** in the **Setup Choices** dialog box. See Setup choices in the section on Installing OTM server software.

2 The **Uninstall Confirmation** dialog box, see Figure 137 on page 262, displays a list of the OTM applications that are currently installed, and asks for confirmation that you want to delete them. Click **Yes** to continue.

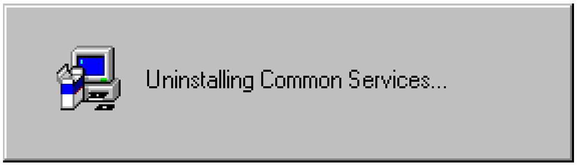
Figure 137
Uninstall Confirmation dialog box



Do you want to remove the following application(s):
Alarm Management
Call Tracking
CCCR
Cons. Rep. Sys.
DECT
ESN ART
Gen. Cost Allc. Sys
ITG IP Phones
ITG IP Telecommuter
ITG IPLine30
ITG ISDN IP Trunks
ITG M1 IP Trunks
LDAP Sync.
Maintenance Window
Station Administration
TBSWEB
Telecom Billing Sys
Traffic Analysis
Web Alarm Mgmt.
Web Common Services
Web Station Admin.
Common Services

3 The status box, see Figure 138, provides a visual indicator of the progress of the uninstall process. Common Services is the last application to be uninstalled.

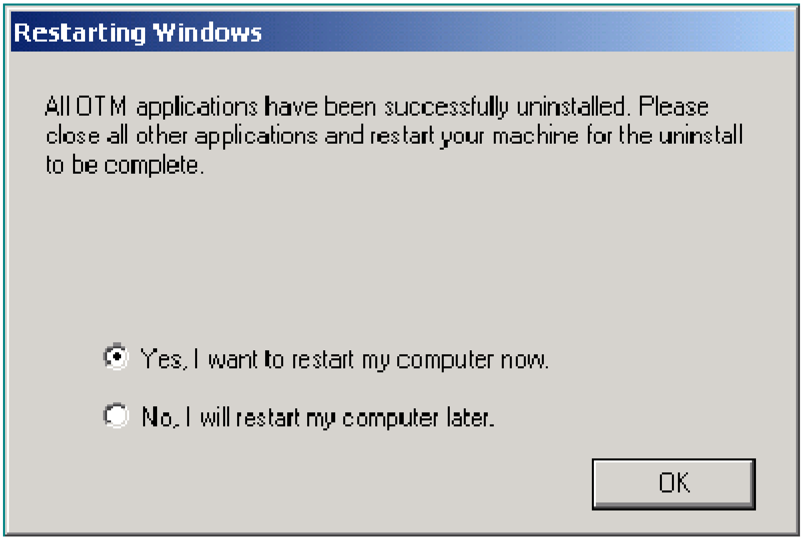
Figure 138
Uninstall status box



Uninstalling Common Services...

4 The Reboot request dialog box appears requesting that you reboot the PC, giving the option of performing the reboot now or later. See Figure 139 on page 263. Select your preference and click **OK** to continue.

Figure 139
Reboot request dialog box



Restarting Windows

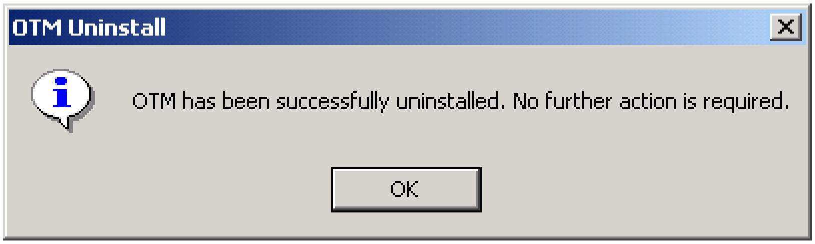
All OTM applications have been successfully uninstalled. Please close all other applications and restart your machine for the uninstall to be complete.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

5 After the PC has been rebooted, the Uninstall complete dialog box appears indicating that OTM has been removed. See Figure 140. Click **OK** to exit.

Figure 140
Uninstall complete dialog box



OTM Uninstall

OTM has been successfully uninstalled. No further action is required.

End of Procedure

Windows 2000 server reference

Contents

This chapter contains information on the following topics:

Overview

This chapter describes an example of Windows® 2000 installation. Due to hardware and software differences, this example may not match your installation.

If a certain component is already correctly installed, then skip the installation of that component.

Installing OTM on Windows 2000 server

Hardware compatibility check

Check all hardware against the documentation available on Microsoft's website at http://www.microsoft.com/windows2000/support/onlinedocs/default.asp.

Running the Windows setup program

Procedure 58
Running the Windows setup program

This procedure shows you how to install Windows server using the setup program:

1. Make sure the first bootup option on CD-ROM in the BIOS is enabled.
2. Insert the Windows server setup CD-ROM into the CD-ROM drive.
3. Boot the system.

4 In the Windows server Setup Welcome dialog box, press Enter to set up the Windows server.

5 In the Windows Licensing Agreement dialog box, press Page Down to go to the bottom of the page, and then choose F8.

6 Press C to create a partition, and then type the size of the partition that you want to create.

7 Use the up and down arrow keys to select the partition created on the first disk in step 6.

8 Press Enter to set up Windows server on the selected partition.

9 Use the up and down arrow keys to select Format partition using the NTFS files system, and then press Enter.

10 Wait while the setup program formats the partition. This takes several minutes.

11 Wait while the setup program copies files to the Windows installation folders. This takes several minutes.

12 Reboot the system.

When the system reboots, press F2 to instruct the system to boot from the hard drive instead of the CD-ROM.

End of Procedure

Installing Windows server components

Procedure 59
Installing Windows server components

Windows server setup continues after the reboot.

1 The Installing Devices dialog box appears. This takes several minutes.

2 The Regional Settings dialog box appears. Select the default values or configure as needed, and then click **Next**.

3 The Personalize Your Software dialog box appears. Enter your name and the name of your organization, and then click **Next**.

4 The Your Product Key dialog box appears. Enter the product key, and then click **Next**.

5 The Licensing Modes dialog box appears. Select the default value, or choose Per server or Per Seat, as appropriate, and then click **Next**.

6 The Computer Name and Administrator Password dialog box appears. Enter the computer name and the administrator password, and then click **Next**.

7 The Windows Components dialog box appears. Select the default values or select specific components, as appropriate, and then click **Next**.

8 The Date and Time Settings dialog box appears. Adjust the Date, Time, and Time Zone, as appropriate, and then click **Next**.

9 Wait for the Network Settings dialog box to appear. This takes several minutes.

10 When the Network Settings dialog box appears, accept the default value, Typical Settings, and then click **Next**.

11 The Workgroup or Computer Domain dialog box appears. Make the appropriate selection, and then click **Next**.

12 Wait while the set up program installs components. This takes several minutes.

13 Wait while the set up program performs final tasks. This takes several minutes.

14 The Completing the Windows Setup Wizard dialog box appears. Click **Finish** to reboot the system.

End of Procedure

Allowing OTM client access without constant server log in (optional)

Procedure 60
Allowing OTM client access without constant server log in (optional)

1 In order to allow OTM client access without being logged in to the server at all times, the following configuration change for Windows server is required:

2 Log in to the Windows server.

3 Go to **Start** > **Programs** > **Administrative Tools** > **Component Services.**

4 From the Component Services window, expand **Computers** > **My Computer** > **COM+ Applications.**

5 Select **OTM Application**, and open the Properties window.

6 Select the **Identity** tab and click on the **This User** radio button.

7 Enter the local administrator account and password.

8 Click **OK**.

Note: This procedure works for all applications except DECT.

End of Procedure

Installing Network Adapter software

Before configuring the network adapters, make sure that the adapters are inserted properly into the slots and RJ45 cables are plugged into the adapters. The Nortel server Subnet Interface card is recommended to install on the top PCI slot and ELAN subnet on the second-from-the-top PCI slot.

Procedure 61
Installing Network Adapter software

1. In Windows 2000 Setup, verify that the Wired to the network check box is checked, and then click **Next.**
2. In the Install Microsoft Internet Information server dialog box, uncheck the box, and then click **Next**.
3. Click **Select** from the List in the Network Adapter dialog box.
4. Click **Have Disk** and insert the CD from the manufacturer (shipped with the network card). Click **OK** and select the appropriate driver from the list. Click **OK** to continue.
5. The next widow appears your LAN card. Since the server has two LAN cards, click on **Select from the list** to install the Nortel server Subnet Interface card driver, and follow the previous step to install the Nortel server Subnet Interface card.
6. In the Network Protocol dialog box, only select **TCP/IP** protocol, and then click **Next** to continue.
7. In the Network Services dialog box, you see the following services:

   - RPC configuration
   - NetBIOS Interface
   - Workstation
   - server

   Click to select the desired services.
8. Click **Next** to install selected components.
9. Click **OK** for Adapter Properties.
10. If the ELAN subnet card is the same type as the previously installed Nortel server Subnet Interface card, the following message may appear: “A network card of this type is already installed in the system. Do you want to continue?” Select **OK**.
11. The Adapter Properties dialog box appears for the second LAN card. Click **OK** to continue.

End of Procedure

Configuring TCP/IP

See “Typical configurations” on page 300" in Appendix A for information on different network configurations that are possible with OTM.

Procedure 62
Configuring TCP/IP

Follow the procedure below to configure TCP/IP settings on a Windows server:

1 Choose **Start > Settings > Network and Dialup Connections**.

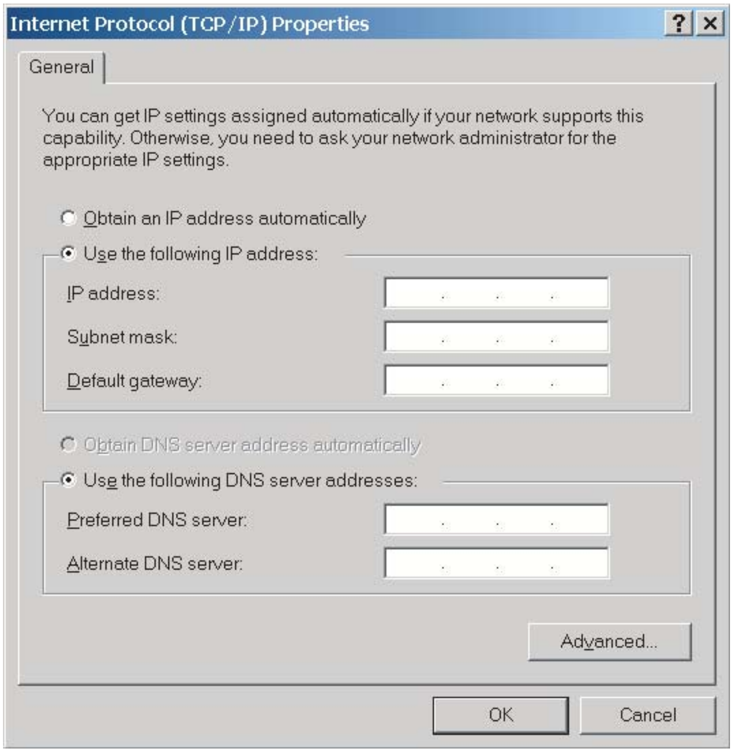
2 In the Network and Dialup Connections dialog box, right-click the Local Area Connection icon, and then select Properties.

3 In the Local Area Connection Properties dialog box, click to select Internet Protocol (TCP/IP), and then click **Properties**.

The Internet Protocol (TCP/IP) Properties dialog box appears. See Figure 141 on page 270.

Note: Ensure that the DHCP IP address is a static address as the host name and IP address are used for client licencing . If the client's IP address changes, the client will not be able to log in until the licence file has been adjusted.

Figure 141
Internet Protocol (TCP/IP) Properties dialog box



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

4 If you have a DHCP server and you want to configure the IP address from the DHCP server, select the Use the following IP address radio button. Enter the IP address, Subnet Mask, Default gateway, and DNS server information.

For PCs with two adapters:

- Select adapter “[1]…” and enter the IP Address, Subnet Mask, and Default Gateway for the Nortel server Subnet Interface connection.

- Select adapter “[2]…” and enter the IP Address, Subnet Mask, and Default Gateway for the ELAN subnet connection.

To enter WINS server information, click Advanced in the Internet Protocol (TCP/IP) Properties dialog box.

Click **OK**.

5 Reboot the system.

End of Procedure

Configuring OTM Dual Network Interface

The OTM server (or client) may have a second network interface card (NIC) installed to connect to the ELAN subnet of a managed system. This can result in the multicast traffic being sent on the ELAN rather than on the intended Nortel server Subnet (formerly referred to as the CLAN). The ELAN subnet must be protected from such traffic.

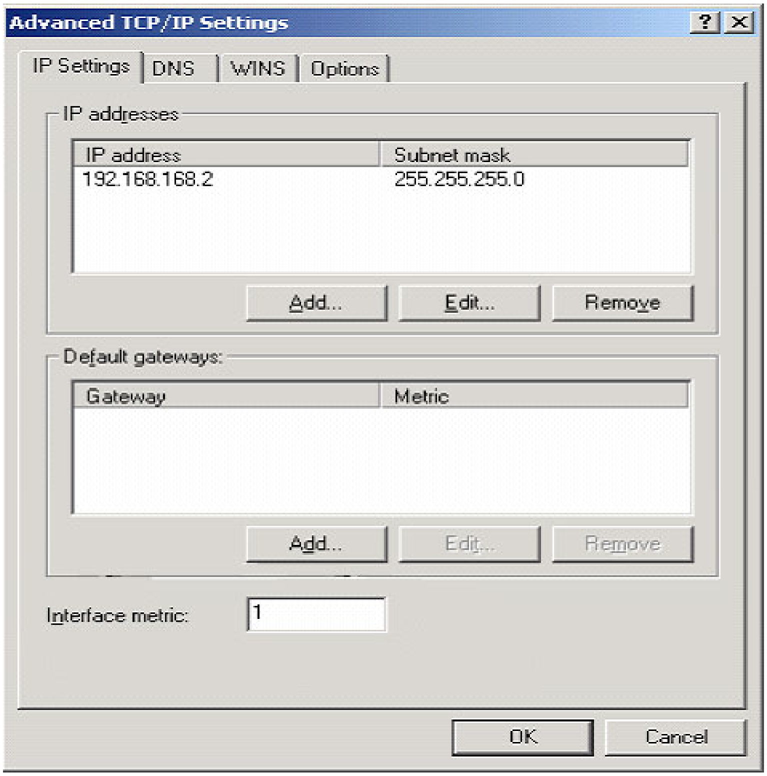
To prevent this type of multicast traffic, the metric value of the ELAN network interface card must be modified so that it is greater than that of the network interface card connecting to the Nortel server Subnet. This will cause the server to prefer the Nortel server Subnet network interface for multicast traffic, rather than the ELAN network interface.

The binding order of the network interfaces is also important; the Nortel server Subnet network interface should be first in the binding order. Network services not used on the ELAN subnet are disabled as well.

Procedure 63
Configuring OTM Dual Network Interface

1. Right- click on **My Network Places,** and select **Properties**.
2. Right- click on the ELAN network interface card, and select **Properties**. Ensure that the **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** checkboxes are unchecked. If not, then uncheck and save the changes.
3. Select **Internet Protocol (TCP/IP)** and then click **Properties**. The IP Address and Subnet mask should be set. The Default gateway field must be left empty to avoid transmission of unintentional traffic on the ELAN subnet.
4. Click **Advanced**. The **Advanced TCP/IP Settings** dialog box appears. See Figure 142 on page 272.

Figure 142
Advanced TCP/IP Settings dialog box



IP address	Subnet mask
192.168.168.2	255.255.255.0

Gateway	Metric

Interface metric: 1

5 In the “IP Settings” tab, modify the “Interface Metric” value to a value greater than that of the Nortel server Subnet network interface. Click **OK** to save all changes.

6 Alter the binding order of the Nortel server Subnet network interface to a number-one postion by completing the following procedure:

a. Select **Start > Settings > Control Panel**.

b. Double-click **Network and Dial-up Connections**.

c. On the Advanced menu, click **Advanced Settings**. The Connections box appears the network adapters.

d. Select the Nortel server Subnet network interface adapter.

e. Use the arrows on the right side of the box to move the adapter ahead (higher than) of the ELAN network interface adapter (if necessary), and then click **OK**.

f. If you are prompted to restart the computer, click **Yes.**

7 Ensure that all changes have been saved and the server restarted. When the server restarts, check that all settings have been applied. Launch a command prompt window and check the routing table using the "route print" command. The interface metric value should have changed.

Installing a modem

Procedure 64
Installing a modem

Follow the procedure below to install a modem on a Windows server:

1 Choose **Start > Settings > Control Panel**.

2 Double-click the Phone and Modem Options icon.

3 In the Phone and Modem Options dialog box, click the Modems tab.

4 If the modem on the computer is not already installed, click **Add**.

If the modem is attached to the computer, Windows can detect and install a modem automatically.

5 In the Install New Modem dialog box, click **Next** to continue.

6 If the system is unable to detect the modem, you must insert the modem manufacturer's disk that came with the modem, and then select Have disk to install.

7 If the system does not have a modem attached, select Standard 28800 bps Modem from the list.

8 Click **Finish** to close the dialog box.

End of Procedure

Installing Remote Access Service

Procedure 65
Installing Remote Access Service

Follow the procedure below to install Remote Access Service (RAS) on a Windows server:

1 Choose **Start > Settings > Network and Dialup Connections**.

2 Double-click the **Make New Connection** icon.

3 In the Network Connection Wizard welcome dialog box, click **Next**.

4 In the **Network Connection Type** dialog box, select **Accept incoming connections**, and then click **Next**.

5 In the **Devices for Incoming Connections** dialog box, select the appropriate connection device, and then click **Next**.

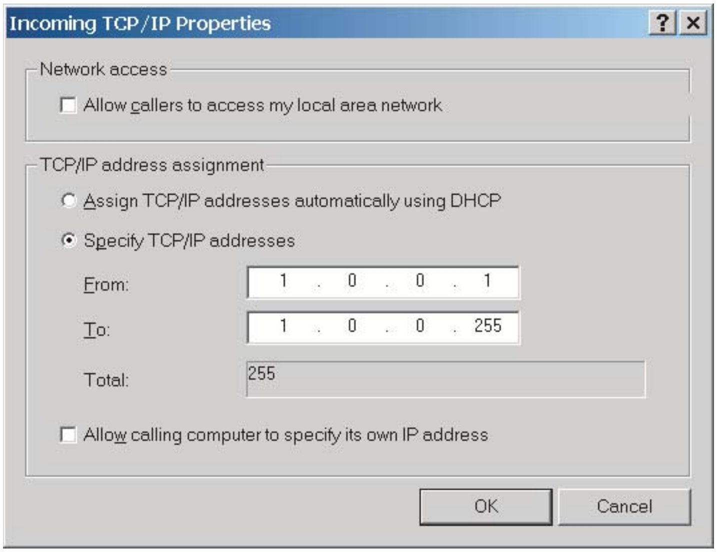
6 In the **Incoming Virtual Private Connection** dialog box, select **Do not allow virtual private connections** check box, and then click **Next**.

7 In the **Allowed Users** dialog box, select the users that are allowed to connect to the server, and then click **Next**.

8 In the Networking Components dialog box, select **Internet Protocol (TCP/IP)**, and then click **Properties**.

The Incoming TCP/IP Properties dialog box appears. See Figure 143.

Figure 143
Incoming TCP/IP Properties dialog box



Incoming TCP/IP Properties

Network access

□ Allow callers to access my local area network

TCP/IP address assignment

○ Assign TCP/IP addresses automatically using DHCP

● Specify TCP/IP addresses

From: 1 . 0 . 0 . 1

To: 1 . 0 . 0 . 255

Total: 255

□ Allow calling computer to specify its own IP address

9 In the **Incoming TCP/IP Properties** dialog box, clear the **Allow callers to access my local area network** check box. Click the Specify TCP/IP address radio button. Enter the initial range as From 1. 0 . 0 . 1 to 1 . 0 . 0 . 255, and then click **OK**.

10 In the Networking Components dialog box, click **Next**.

11 In the Completing the Network Connection Wizard dialog box, type the connection name, and then click **Finish**.

End of Procedure

Testing network cards

Test the network cards after you complete the Windows server installation.

Testing the Nortel server subnet interfacet

Procedure 66
Testing the Nortel server subnet interface

Network connectivity can be verified by pinging a server or workstation known to be accessible only via the Nortel server subnet. This could be an OTM web client or other server.

From **Command Prompt** window on the OTM server, enter the command **`ping <IP address>`**.

End of Procedure

Testing the Embedded LAN interface

Procedure 67
Testing the Embedded LAN interface

Network connectivity can be verified by pinging a system on the ELAN. This could be the ELAN Network interface IP address of a Call Server, for example: From a Command Prompt window on the OTM server, enter the command **`ping <IP address>`**.

End of Procedure

Appendix A: OTM engineering guidelines

Contents

This appendix contains information on the following topics:

Overview

This appendix provides a set of guidelines to help you determine the configuration and distribution of OTM servers within a network to efficiently manage CS 1000 and Meridian 1 systems.

Capacity factors

This appendix examines the following areas where capacity is a factor:

- Features running on the OTM server and their impact to its resources, such as CPU usage, physical memory (RAM), and disk storage
- web and OTM clients and their impact on OTM server resources
- web-based Station Administration Write capability (that is, performing Station updates over the web) and its impact on the OTM server
- CS 1000 and Meridian 1 systems and their impact on OTM server resources
- Communications between the OTM server and CS 1000 and Meridian 1 systems, OTM/web clients, LDAP server, and so on, and their impact on the network to which they are connected.

The Billing applications result in a processor load that is not possible to predict. The exact impact depends on several factors, including types of reports being generated and quantity of data being merged. It is not possible to derive a general formula to predict the impact of these applications. Nortel recommends that these applications be run during off-hours, and that they not be run in parallel with other resource-intensive applications.

Impact analysis

Analysis was performed on the majority of OTM features. To simplify analysis, only those features that impact these resources are highlighted here.

Based upon this analysis, recommendations are made as to:

- The resources required on the OTM server
- The number of clients and systems that can be connected to a single OTM server
- Network bandwidth and routing considerations

  Analysis of the results of benchmark testing are presented in Table 17 on page -296, Table 18 on page -307, and Figure 149 on page -310. The tables can be used to calculate the resources and connections possible for various OTM server usage scenarios.

- Table 17 highlights PC performance for several OTM applications.
- Table 18 highlights the peak and average transfer rates for various OTM activities.
- Figure 149 presents a graphical representation of station response time compared with round-trip time (RTT).

To aid in this process, this appendix analyzes four typical OTM server configurations. Use these configurations as examples and the raw table data to extrapolate configurations specific to a given customer/distributor setup.

These guidelines provide minimum PC configurations for the OTM server, OTM client, web client, and OTM running in a stand-alone mode.

Hardware and software comparisons

Table 13 shows a list of machine types for Meridian 1 with CS 1000 Release 4.5.

Table 13
Hardware Machine Type for Meridian 1 hardware with CS 1000 Release 4.5

	When 'Signaling server' checkbox in 'Network' page is cleared		When 'Signaling server' checkbox in 'Network' page is selected	
Hardware with CS 1000 Release 4.5	**System Type**	**Machine Type**	**System Type**	**Machine Type**
11C/Mini	Meridian1	11C / 11C Mini	Communication server 1000	CS 1000M Small System
51C 060	Meridian1	51C 060	Communication server 1000	CS 1000M HG 060
51C 060E	Meridian1	51C 060E	Communication server 1000	CS 1000M HG 060E
61C 060	Meridian1	61C 060	Communication server 1000	CS 1000M SG 060
61C 060E	Meridian1	61C 060E	Communication server 1000	CS 1000M SG 060E
61C PII	Meridian1	61C PII	Communication server 1000	CS 1000M SG PII
81, 81C 060	Meridian1	81, 81C 060	Communication server 1000	CS 1000M MG 060
81, 81C 060E	Meridian1	81, 81C 060E	Communication server 1000	CS 1000M MG 060E
81C PII	Meridian1	81C PII	Communication server 1000	CS 1000M MG PII

Software limits

Co-residency support

Table 14 shows the current list of available co-residency support for OTM.

Table 14
Co-residency support (Part 1 of 7)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
HPUX 11.0	Netscape 4.79 English	N/A	N/A	ONMS 10.1/ONMS 10.2
Solaris 2.8	Netscape 4.79 English	N/A	N/A	ONMS 10.1/ONMS 10.2
XP Pro	IE 6 English	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in English	2.2 English client or standalone	• PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus Corporate Edition 8.0 • McAffee VirusScan 8.0 • NetIQ Agent
2000 Pro	IE 6 English	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in English	2.2 English client or standalone	• ONMS 10.1/ONMS 10.2 client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (English) • SECC 4.2 SMI Workbench (English), Symposium web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0, • PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus Corporate Edition 8.0 • McAffee VirusScan 8.0 • NetIQ Agent

Table 14
Co-residency support (Part 2 of 7)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 server	IE 6 English	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in English	2.2 English server installation	• PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus Corporate Edition 8.0 • NetIQ Agent • McAfee VirusScan Enterprise 8.0
2000 Pro in French	IE 6 French	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in French	2.2 French client or standalone	• ONMS 10.1/ONMS 10.2 client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (French) • SECC 4.2 SMI Workbench (French) • Symposium web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0 • PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton AntiVirus Corporate Edition 8 • Norton Antivirus 2003 (Standard and Professional) • McAfee VirusScan 8.0 • NetIQ agent

Table 14
Co-residency support (Part 3 of 7)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 Pro in German	IE 6 German	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in German	2.2 German client or standalone	• ONMS 10.1/ONMS 10.2 client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (German) • SECC 4.2 SMI Workbench (German) • Symposium web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0 • PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus 2003 (Standard and Professional) • McAfee VirusScan 8.0 • NetIQ agent

Table 14
Co-residency support (Part 4 of 7)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 Pro in Japanese	IE 6 Japanese	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Japanese	2.2 English client or standalone	• ONMS 10.1/ONMS 10.2 client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (Japanese) • SECC 4.2 SMI Workbench (English) • Symposium web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0 • PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus 2003 (Standard and Professional) • McAfee VirusScan 8.0 • NetIQ agent

Table 14
Co-residency support (Part 5 of 7)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 Pro in Chinese Simplified	IE 6 Chinese Simplified	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Simplified Chinese	2.2 English client or standalone	• ONMS 10.1/ONMS 10.2 client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (Simplified Chinese) • SECC 4.2 SMI Workbench (English) • Symposium web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0 • PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus 2003 (Standard and Professional) • McAfee VirusScan 8.0 • NetIQ agent

Table 14
Co-residency support (Part 6 of 7)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 Pro in Spanish	IE 6 Spanish	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Spanish	2.2 English client or standalone	• ONMS 10.1/ONMS 10.2 client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (Spanish) • SECC 4.2 SMI Workbench (English) • Symposium web Center Portal Administrator client 4. • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus 2003 (Standard and Professional) • McAfee VirusScan 8.0 • NetIQ agent
2000 Pro in Brazilian	IE 6 Brazilian	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Brazilian	2.2 English client or standalone	• ONMS 10.1/ONMS 10.2 client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (English) • SECC 4.2 SMI Workbench (English) • Symposium web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus 2003 (Standard and Professional) • McAfee VirusScan 8.0 • NetIQ agent

Table 14
Co-residency support (Part 7 of 7)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 server in Japanese	IE 6 Japanese	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Japanese	2.2 English server installation	• PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus 2003 (Standard and Professional) • NetIQ agent
2000 server in Simplified Chinese	IE 6 Simplified Chinese	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Simplified Chinese	2.2 English server installation	• PC Anywhere 11.0, "Timbuktu Pro 7.0" • Norton Antivirus 2003 (Standard and Professional) • NetIQ agent
web clients:				
Any PC OS listed in above table which supports IE 6	IE 6	N/A	OTM 2.2 web client (Administrat or UI)	• CallPilot 2.5/3.0 web clients (Administrator CallPilot web client) on IE 6 • SCCS 4.2/5.0 web Admin client 4.5/5.0 on IE 6 • Symposium Agent (Administration Workstation) on IE 6 • Symposium Agent Greeting 2.0 on IE 6 • BCM 3.5 web Management Interface on IE 6 • Nortel Hospitality Integrated Voice Services version 1.17 web browser management tool on IE 6.
Any PC OS listed in above table which supports IE 6	IE 6	N/A	OTM 2.2 web client (Desktop UI)	• CallPilot 2.5/3.0 web clients (My CallPilot) on IE 6 • SCCS 4.2/5.0 web client 4.5/5.0 (Agent UIs) on IE 6 • Symposium Agent Greeting on IE 6 • Integrated Voice Services version 1.17 web browser management tool on IE 6.

Hard-coded limits

This section lists the hard-coded limits in the OTM software.

Table 15 outlines the maximum value for many of the parameters associated with the various components of OTM.

Table 15
OTM capacity parameters (Part 1 of 5)

Parameter	Maximum Value
Windows Common Services	
Maximum number of Sites that can be created on an OTM server	3 000
Maximum number of MG 1000B systems can be created under a specific site	256
Maximum number of synchronization/Update tasks (number of Log Windows) that can be executed at the same time	5
Number of Customers	100
Range of DN	0-9999999
Maximum number of Survivable Expansion Cabinet	4
Maximum number of modem scripts that can be created	3 000
Windows Common Services	
Maximum number of application jobs that can be scheduled in the Scheduler application	2 000
Max String Length for:	
Site name	31
System name	31
Address	44
City	24
State/Province	24
Country	24
Zip/Postal Code	16
Comments	255
IP Address	15
Display (CPP profile)	1 000
Timeout (CPP)	60
Phone Number (CPP)	50

Table 15
OTM capacity parameters (Part 2 of 5)

Parameter	Maximum Value
Access ID (CPP)	50
Modem Password (CPP)	50
Modem Installation String (CPP)	50
Issue	99
System ID	16
Maximum Speed Call Lists	8 191
Maximum ACD Agents	1 200
PDT password	16
Customer Name	31
Directory Numbers	24
Customer Password	16
HLOC	9 999
Dial Intercom Group	2 045
User ID	2 045
LDAP	
Maximum number of LDAP Sync Log files that can be created separately	2 000
Number of LDAP entries that can be synchronized at the same time	10 000
Number of entries that can be added from LDAP server to OTM Directory	15 000
Corporate Directory	
Maximum number of customized reports that can be created	2 000
Number of data fields that can be defined into a corporate report	111
Maximum number of reports that can be generated at the same time	1
Maximum string length of all parameters	255 characters
Maximum number of entries in Corporate Directory file uploaded to Large systems (e.g., 61C)	120,000
Maximum number of entries in Corporate Directory file uploaded to Small systems (e.g., CS 1000S)	16,000
Maximum number of entries in Corporate Directory file uploaded to Meridian 1 PBX 11C Chassis	2,000

Table 15
OTM capacity parameters (Part 3 of 5)

Parameter	Maximum Value
Data Buffering and Access (DBA)	
Maximum number of Action records that can be defined in a DBA session	1 000
Maximum number of Rule records that can be defined in a DBA session	1 000
Maximum number of CDRs that can be collected	5 000 000
List Manager	
Maximum number of speed call lists that can be created	8 190
Maximum number of group call lists that can be created	63
Maximum number of group hunt lists that can be created.	8 190
Maximum String length for:	
Speed Call List	
List Name	50
Entry Name	50
Dialed Digits	31
Speed Call List	
Entry Number	999
PLDN	31
Group Call list:	
List Name	50
Entry Name	50
Entry Number	19
Group Hunt List:	
List Name	50
Maximum String length for:	
Group Hunt List:	
PLDN	50
Dialed Digits	31
Entry Name	50
Entry Number	95
Station Administration	
Maximum number of External Parties that can be created	5 000

Table 15
OTM capacity parameters (Part 4 of 5)

Parameter	Maximum Value
Maximum number of Role/Projects that can be created	5 000
Maximum number of employees that can be created	16 000
Maximum string length of all parameters	128 characters
OTM DECT	
Maximum number of DECT Systems	500
Maximum String length for:	
DECT system name	255
Password	Unlimited
IP Address	15
OTM server IP Interface	15
Phone Number	64
PARI (Access Right Identification tab)	8
SARI (Access Right Identification tab)	8
Upstream Manager IP address (Access Right Identification tab)	15
Maintenance Windows	
Maximum number of maintenance commands that can be run at the same time	10
Maximum number of maintenance commands that can be executed at the same time in web Maintenance	10
OTM web	
Maximum number of clients that can log on to the Administration page of the same OTM server at the same time	5
OTM web	
Maximum number of clients that can log on to the web EndUser page of the same OTM server at the same time	20
Maximum number of sessions that can be controlled by OTM web server	1 000
Maximum number of telephones that can be assigned to an end user	200
Data Buffering and Access (DBA)	

Table 15
OTM capacity parameters (Part 5 of 5)

Parameter	Maximum Value
Maximum number of systems	256
Corporate database	
Maximum number of organizational levels	20
Virtual Terminals	
Maximum number of Virtual Terminals that can be enabled at one time	256
Billing applications (TBS, CCCR, CRS, and GCAS)	
Maximum number of call records per costing configuration in TBS	2 500 000
Maximum number of call records for CCCR **(across all systems)**	5 000 000
Maximum number of call records for GCAS	4 000 000
Maximum number of call records for CRS (TBS & GCAS combined)	2 500 000
Maximum number of managed systems for TBS Billing General and TBS Billing Enhanced (TBS,CCCR,CRS, and GCAS)	10
Maximum number of lines in a PBX for TBS Billing General and TBS Billing Enhanced (TBS,CCCR,CRS, and GCAS)	3500
Maximum number of Consolidated Multi-site Reports for TBS Billing General	0
Maximum number of Consolidated Multi-site Reports for TBS Billing Enhanced (TBS,CCCR,CRS, and GCAS) CCCR operates only within a single OTM server and can only be run on an OTMserver or standalone system	5 (CCCR)
Alarm Management	
Maximum number of traps in the circular queue	1360

Rate of alarm production

A single system produces alarms, on average, at the rate of one every ten seconds. This means the queue can hold 3.7 hours worth of alarms from a single system without losing alarm information.

Starting with Release 25 of Meridian 1 system software and in all releases of Communication server 1000 software, there is the capability of filtering traps, on the PBX, based upon their categorization (for example, minor, major, critical, and so on). This can greatly reduce the alarm rate by permitting only major and critical alarms to be sent to OTM.

Filtering increases the number of systems that can be connected. However, when a single system begins having a problem, it begins reporting major/critical alarms at the rate of 1 every 2 seconds. This means that the queue can hold only the last 45-minutes worth of alarms from the offending system, assuming that alarms from the other systems are minimal.

Billing applications sizing guidelines

The OTM billing application is intended for use in small to medium sized customer networks. OTM billing is most suitable for networks which do not require substantial data processing or those with many nodes.

There are two considerations for determining whether OTM billing is suitable for a particular customer network. The first is the size of the largest system for which billing will be used, and the other is the total number of systems in the network. See Table 15 on page 287 for some practical guidelines on determining if the OTM billing application meets your customer's requirements.

When CDR is collected and costed, the Telecom Billing System (TBS) generates a separate Microsoft Access database for each individual costing configuration (PBX system). Each PBX system defined in TBS has a capacity limit of 2.5 million costed call records which is a limitation of the Microsoft Access database used in the billing application. While TBS does not enforce a maximum number of systems that will be supported, we recommend using the above guideline of 10 systems per OTM server configuration to ensure that adequate resources are available. The size of the database determines how often call records are archived in order to ensure that there is adequate capacity to receive additional call records. However, the larger the database, the more often archiving is required to achieve the desired result. The recommended maximum of 3,500 lines per PBX is a conservative limit based upon the assumption that a PBX with 3,500 lines generates approximately 800,000 call records per month. This leads to an archival interval of 12.5 weeks and allows reporting on 3 months of calling activity within a single database. Please note that call record generation varries depending upon how the switch is being used, so having a good understanding of the customers call volume is highly recommended.

The sizing guidelines are provided to help ensure that OTM performs optimally. OTM billing will still operate past these limitations, but with degraded performance. Performance concerns that arise from using OTM past the recommended limitation will not be considered as a product deficiency.

> ***Note:*** The time to cost CDR records and generate reports is directly proportional to the size of the call record database. For larger or busier switches, the response time for costing CDR and generating reports will be slower than with a smaller switch that doesn't generate as many call records.

Operational limits

OTM web interface

Usage of the OTM web interface has the advantages of not requiring installation of the OTM client and providing the ability to access the OTM server from any PC with a web browser. However, using the web interface places a heavier workload on the OTM server. The web Desktop Services Write capability was introduced in OTM 1.1, and provides end users as well as administrators with the ability to configure telephones using a web interface. After a telephone's configuration has been changed and scheduled, the job is placed into the queue of the scheduler.

The scheduler executes the jobs in the queue one by one. This impacts the throughput of the system. There is a delay between the time that the job is scheduled and the time that the job is finished. While the job is being executed, the peak CPU usage may approach 100 percent causing a performance degradation to other applications.

web station

web Station Write capability requires more OTM server resources than earlier versions of OTM without this capability. For example, a station change performed through the web interface takes up to 27 seconds of CPU time (2 seconds for finding, 3 seconds for changing, and 22 seconds for transmitting), while a change through the Windows Station Administration application requires only 23.8 seconds of CPU time (1 second for finding, 0.8 seconds for changing, and 22 second for transmitting).

Performance of station administration activities primarily through the web interface places a slightly larger workload on the OTM server. For example, in a system with 10,800 lines and a daily change rate of 1%, Add/Move/Change activity through the web interface consumes aproximately 27.0 percent of CPU usage compared to only 23.8 percent if performed using the Windows interface.

web Desktop Services for end-users

When you configure the write capability for end users in web Desktop Services, you also place a higher workload on the OTM server.

However, the ability for end users to make changes may decrease the need for the network administrator to make changes; therefore, the impact of configuring the write capability for end-users in web Desktop Services may not be significant in certain configurations.

web support on server and Workstation platforms

Table 16 outlines the differences observed in web support when OTM is running on server grade platforms and workstation platforms.

Table 16
web support on servers and workstations

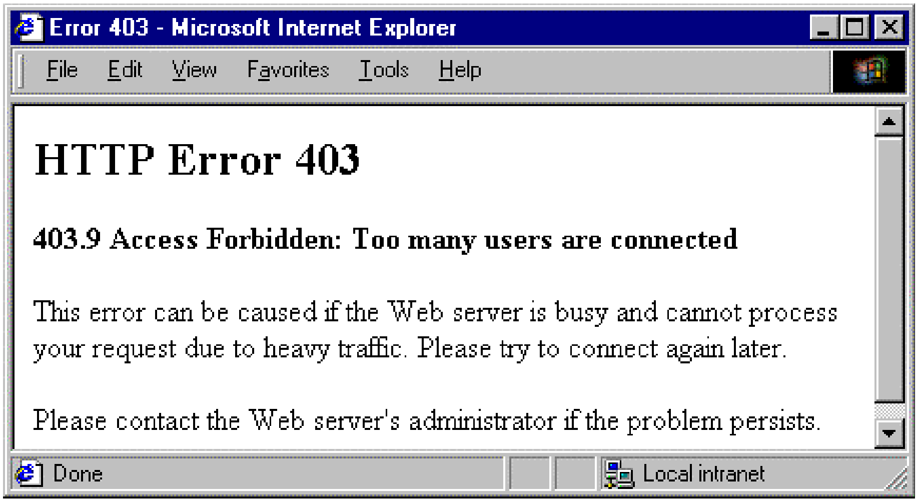
	IIS on Windows 2000 server	PWS on Windows 2000 Professional
Concurrent Internet Explorer sessions	Only limited by OTM capacity	5
Concurrent Netscape Navigator sessions	Only limited by OTM capacity	2
Restricted Access by IP address and domain name	Yes	No

Personal web server (PWS) is only intended to provide low-volume web publishing capability. Performance degrades with increased traffic and complex web pages or Java applications.

The number of sessions supported by PWS is based on a ten-connection limit. Internet Explorer uses two connections per session, while Netscape Navigator uses between four and six connections depending on the size of the web page.

When additional clients attempt to access web Services and there are no available connections, an error message appears. See Figure 144 on page 295.

Figure 144
Too-many-users-are-connected error message


Error 403 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Done
Local intranet

HTTP Error 403

403.9 Access Forbidden: Too many users are connected

This error can be caused if the Web server is busy and cannot process your request due to heavy traffic. Please try to connect again later.

Please contact the Web server's administrator if the problem persists.

Modems

A modem connection between the OTM client and the OTM server is used for the command line interface (CLI) and web applications. The OTM server can operate as a terminal server, and the OTM client uses the CLI to access the Meridian 1 and CS 1000 systems. Nortel recommends that you migrate to web applications and access OTM features in a client/server configuration using a modem connection.

Operational testing

The test setup was:

- A 600 MHz Pentium II with 512 MB of memory and ATAPI hard disk interface
- A Meridian 1 PBX 61C \Meridian 1 PBX 81C, assumes that 1% of a total of 1000 lines are changed on a daily basis by the network administrator
- For an Meridian 1 PBX 11C Cabinet or CS 1000S system, decrease CPU usage by a factor of 2 and increase elapsed time by the same factor for those features that interact with the system (for example, Station Update, but not Cost Report).

- A 100 MB network

Table 17 lists those OTM applications that have a significant impact on the performance of the OTM server PC. The table lists CPU utilization and elapsed time statistics, as appropriate, when connected to a single system.

Table 17
PC performance by application

Application	Real Time (CPU)		Elapsed Time
	Peak	Average	
Station Administration Add/Chg/Del		2.2%	
Station Reconcile with Meridian 1 system	100%		1 record/3 seconds
web Station Administration	100%		1 record/27 seconds
web Desktop Services write capability for end users	100%		1 record/27 seconds
web Admin		Negligible	
Alarm Monitor	2%	Negligible	
DBA - CDR Collection	6%	3%	
DBA - Traffic Collection	1%	0.5%	
LDAP Sync1	100%		10 records/second
Parsing CDR File	100%		40 records/second
Cost Report	100%		40 records/second
OTM client (Station Update)	4%		1 record/5 seconds

1LDAP Sync testing was based upon the use of an LDAP server dedicated for this testing. Since OTM does not control the LDAP server used in the customer network, the server response time is likely to be less. This server's resources are impacted by factors for the LDAP server, such as processor speed, other uses for LDAP server (for example, Corporate Directory), other LDAP clients, and other services running on the same platform.

PC hardware

This section describes the PC hardware requirements necessary to run OTM optimally. Use the guidelines provided in the sections “Physical memory” on page 297, “Hard disk” on page 298, and “Processor speed” on page 299:

See “OTM hardware requirements” on page 39 for the following information:

- Add additional serial interface cards as needed.
- Calculate disk storage requirements based on applications usage.

- Implement a backup and restore strategy.
- Follow regular maintenance instructions as documented for OTM features to maintain the integrity and capacity of the hard disk.
- Add disk redundancy as required.
- Increase performance by:
  - Adding more system memory
  - Utilizing a faster hard disk or SCSI interface, or both
  - Using a faster CPU
- Scale your PC for future growth, and utilize a PC that:
  - Has a reserve PCI Card slot for a SCSI Interface Card (See "Hard disk" on page -298 for details.)
  - Has a spare storage bay and power for adding an internal hard disk
  - Can accommodate increasing the memory capacity to 1GB or greater (Most PCs have 2 to 4 memory card slots that can accommodate DIMMS of various capacity.)

Response-time testing is based upon the recommended configuration, not the minimum configuration. Response-time performance is only supported on the recommended configuration.

Physical memory

The amount of physical memory installed on the server is critical in achieving maximum performance on the PC. Microsoft Windows systems have a feature called Virtual Memory. Virtual Memory allows the PC to continue running programs that require more memory than there is physical memory available. It borrows memory using a memory-swapping scheme from available space on the main hard disk. Although this feature permits the PC to perform operations without worrying about running out of physical memory and, thus, crashing the computer, it sacrifices performance of these operations by requiring access of the hard disk while memory swapping. This degrades performance because:

- Physical memory access is much faster than disk access.
- Accessing the disk while memory swapping steals disk resources away from applications that need to read and write to the hard disk.

The OTM server software and the Windows server software require approximately 900 MB without active features. The minimum server memory is 512 MB.

The amount of memory does not grow significantly as features are running and windows are opened.

The one exception to this is OTM client access. Each OTM client connection to the OTM server requires an additional 3 MB of memory. For large configurations, such as 100 systems and 50 OTM clients, an additional 150 MB of memory is required.

Hard disk

Disk performance

Much of the time spent by OTM Features is in reading and writing data to the hard disk. Features that spend a significant percentage of their time accessing the disk are called disk-intensive applications. For these features, the access time is critical in terms of the time it takes for a feature to complete an operation.

OTM disk-intensive applications analyzed in this document include:

- CDR and traffic collection
- TBS report generation
- Simultaneous Update of Station Data

  Station Update from a single system is not affected by disk performance, as the speed of transmission from the system is slower than the PC accessing its disk.

- web/OTM client Station Access

"Physical memory" (page -297) recommends a hard disk using the ATAPI interface. It also recommends a single hard disk.

To improve performance you can:

- Use the fastest Ultra-Wide SCSI Interface (15K RPM).

  Disk performance increases by a factor of 2 or better. This can translate to an increase in feature performance (reduce elapsed time and increase simultaneous operations) by 50 percent or better.

  SCSI disk drives come in various speeds.

- Add a hard disk to store OTM Data separate from the OS and Programs.

  If the server PC being used is using an ATAPI interface for its main disk, C:, then installing a SCSI interface card and second hard disk to store OTM Data can achieve the majority of the SCSI performance increase.

Disk size

The OTM server software and the Windows server software requires approximately 900 MB without OTM data or active features.

You must reserve approximately 300 MB of disk space for virtual memory and normal OS operations.

CDR = 250 bytes per record, at peak rates over a one-day period, this creates a 700 MB file.

Station = approximately 500 kb per 100 telephones. From the example in Table 20 on page 321 and Table 21 on page 321:
Disk space = 500 kb/100 telephones*10,000 lines = 50 MB of disk space.

Directory = approximately 80 kb per 100 records. From the example in Table 20 on page 321 and Table 21 on page 321:
Disk space = 80 KB/100 telephones * 10,000 lines = 8 MB of disk space.

Processor speed

The 600 MHZ CPU recommended is sufficient for the maximum configurations presented here.

An increase in CPU power does not, by itself, greatly increase the capacity of the server.

The PC is so I/O bound, from accessing memory to accessing the hard disk, that a two-fold increase in CPU power may result in only a 10 percent increase in OTM capacity.

Replacement of the motherboard, not just the CPU chip, can further increase CPU performance, since the newer motherboard is designed to take advantage of the high processor speeds (for example, faster CPU bus, faster memory, and so on). The PC is still heavily bound to disk access and network speeds.

Windows XP systems may perform slightly slower than Windows 2000 systems of a similar hardware and software configuration due to the nature of the Operating System.

Network bandwidth

Typical configurations

OTM interface access

While the connection from OTM to the managed systems may be either serial or an IP connection, the OTM applications may be accessed by a variety of means:

- The Windows GUI and web interfaces can be used directly on the OTM server.
- Remote users can dial up to the OTM server and use CLI to access the Communication server 1000 and Meridian 1 systems.
- OTM web clients can also be used to connect to the OTM server.
- For full access to OTM features, the OTM client GUI interface can be used.
- Connect to the OTM server / client using a supported remote access software package (e.g., pcAnywhere). This is particularly useful if OTM clients cannot be deployed remotely due to bandwidth limitations.

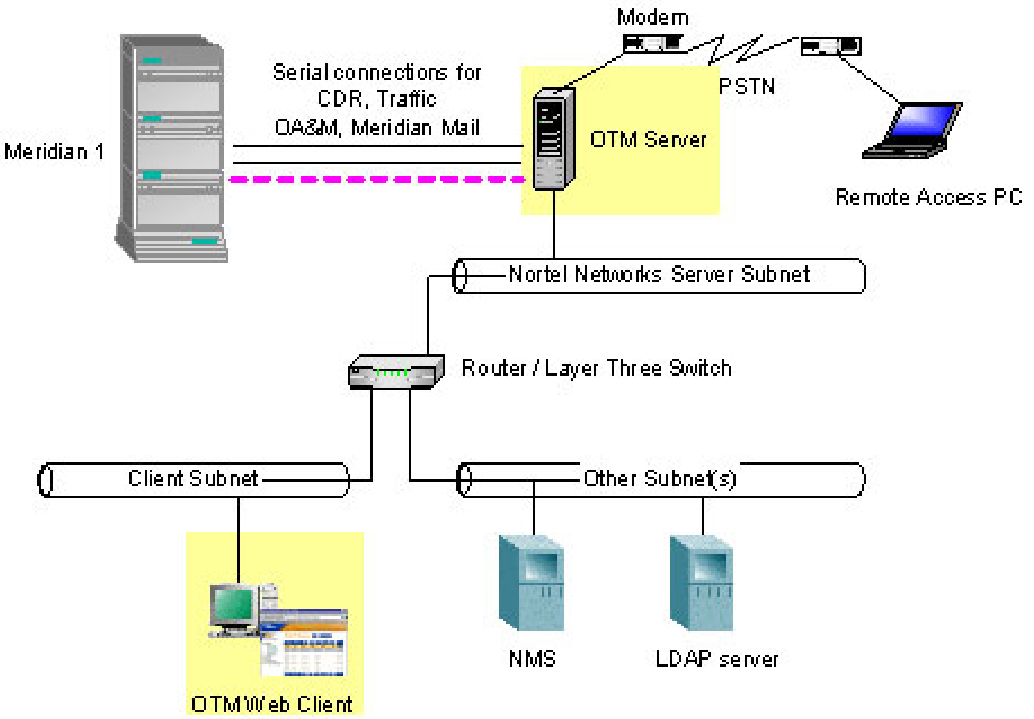
Serial connections to systems

Figure 145 shows how OTM connects to systems that do not support Ethernet. In this scenario, OTM is connected to these systems through their serial ports. Physical limitations on serial connections limit OTM to be placed within 15.24 meters (50 feet) of these systems to minimize noise, which can cause transmission errors. It is also possible for the serial connection to be established over a modem connection. Note that some OTM applications cannot work over a serial connection. For more information, see Table 9: “CS 1000 and Meridian 1 software requirements” on page 49.

The diagram only shows the OTM server, but it is possible for an OTM client to be used. The OTM client requires the same serial connections to the managed systems as the OTM server. The usual limitations of the OTM client apply, such as the need for a high bandwidth connection between the OTM client and the OTM server.

It is possible for the same OTM PC to have serial connections to some systems and IP connections to others.

Figure 145
Connecting OTM to legacy systems (pre-Ethernet)



IP connections to systems

IP connection overview

The OTM solution consists of the OTM server, OTM clients, and OTM web clients. These may be connected in several different configurations. The particular configuration chosen will depend on the tasks to be performed and the network environment.

The following are some of the considerations when deciding on the configuration:

- Are there multiple administrators? Do they require full administration capabilities available with OTM clients, or will the web client functionality be sufficient? The answers to these questions will determine the need for OTM clients.

- The OTM clients connection to the OTM server must have high bandwidth and low Round Trip Time (RTT) characteristics, as documented in the "OTM server and clients overview" on page 39 and, in this appendix, "Network bandwidth" on page 300. Since a WAN connection is not generally suitable this affects the placement of OTM clients.
- The OTM clients require connections to the systems they are managing.
- The OTM server requires connections to the systems if the web client is used or if applications are run on the OTM server (for example, DBA collection of CDR, Station administration by the server Windows GUI interface). Note that if OTM clients are being used, then the connection to the systems is directly from the OTM clients, not through the OTM server.
- The number of systems are being administered by OTM, and what network connectivity is available to these systems. A key point is that a high quality connection is required between the OTM server and OTM clients. On the other hand, the connection between the OTM server and web clients or between the OTM server and managed systems requires significantly lower bandwidth, and most WAN connections should be adequate.

Data networking guidelines

The Data Networking NTP *Converging the Data Network with VoIP* (553-3001-160) gives an overview of all network connections, together with guidelines for their usage. It is important to understand and follow the recommendations contained in it. Only a few key points are mentioned here and the Data Networking NTP should be consulted for details.

- If it is planned to connect the ELAN subnet to the enterprise IP network, a layer three switch or router capable of packet filtering MUST be used to separate the ELAN subnet from the enterprise IP network. The packet filter MUST be configured to prevent broadcast, multicast and unauthorized traffic from entering the ELAN subnet.
- If the ELAN subnet is connected to the enterprise IP network without a packet filtering router, the system's call handling ability may be adversely affected. It is recommended to use a layer two or layer three Ethernet switch for all subnets. This is particularly important on the ELAN subnet when other application servers (e.g., SCCS) are present. The use of shared media hubs can result in adverse system impact under some conditions.

ELAN connection options

The OTM server and OTM client require connectivity to the ELAN subnets of the managed systems. There are two choices for this ELAN configuration:

- The OTM server or client is connected only to the Nortel server subnet (or another subnet of the customer’s Enterprise IP network) and has a routed connection to the ELAN subnets of managed systems. This is the more flexible and preferred configuration.
- The OTM server or client has a network interface that connects directly to the ELAN subnet. A second network interface is also present to connect to the Nortel server subnet. This is referred to as a Dual NIC configuration. Such a setup is suitable if there is only one OTM PC (for example, server but no OTM clients) that requires access to the ELAN subnet. Note that if multiple systems are being managed, the ELAN Network interface on the OTM server or OTM client only allows access to a single ELAN subnet, and the other ELAN subnets have to be accessed by a routed connection from the Nortel server subnet.

OTM clients that also serve as desktop PCs will generally have a routed connection to the ELAN subnets of the managed systems since they are located on the client subnet.

In making the decision regarding which configuration to choose, a factor is whether a routed connection to the ELAN subnet is required for other purposes (for example, the CS 1000 Call Servers send traps directly to an NMS).

ELAN and Nortel server subnet connectivity requirements

Connectivity from the OTM server or client to the ELAN is required for the following operations:

- All system management, configuration, and maintenance of Meridian 1 and CS 1000 devices. Several protocols may be used (e.g., RLOGIN, SNMP).
- Access is required from the OTM server / client to the Signaling server and Voice Gateway Media Card ELAN interfaces (e.g., to pull OM reports for IP Telephony).
- Access from the OTM client or web client for Element Manager access when launched from the OTM Navigator.

Connectivity from the OTM server or client to the Nortel server subnet is required for the following operations:

- If an ELAN Network interface is not present to the ELAN subnet of any managed system, then a routed connection is required from the Nortel server subnet interface to the ELAN subnet.
- OTM client access to the OTM server. Due to the high bandwidth requirements of this connection it is important that the OTM client to OTM server connection not be made via the ELAN subnet.

- web client access to the OTM server.
- Access by a remote access software package (e.g., pcAnywhere).
- LDAP synchronization with the customer LDAP server.
- Forwarding of SNMP traps to a NMS (could be just OTM traps and/or notification traps for managed systems events).

OTM network configuration scenarios

The following are some typical OTM configuration scenarios:

Standalone OTM server

This is the simplest configuration, consisting of an OTM server with no OTM clients. There may be optional web clients. There are two possible setups:

- The server has the Dual NIC configuration, with a dedicated ELAN subnet network interface. Generally only a standalone OTM server that is managing a single system will be set up with an ELAN Network interface. Figure 146 on page 305 illustrates this configuration.
- Routed connections are used from the OTM server to the ELAN subnets of managed systems (via the Nortel server subnet). This configuration is preferred over the Dual NIC configuration. Figure 147 on page 305 illustrates this configuration.

Figure 146
Standalone OTM server with Dual NIC configuration

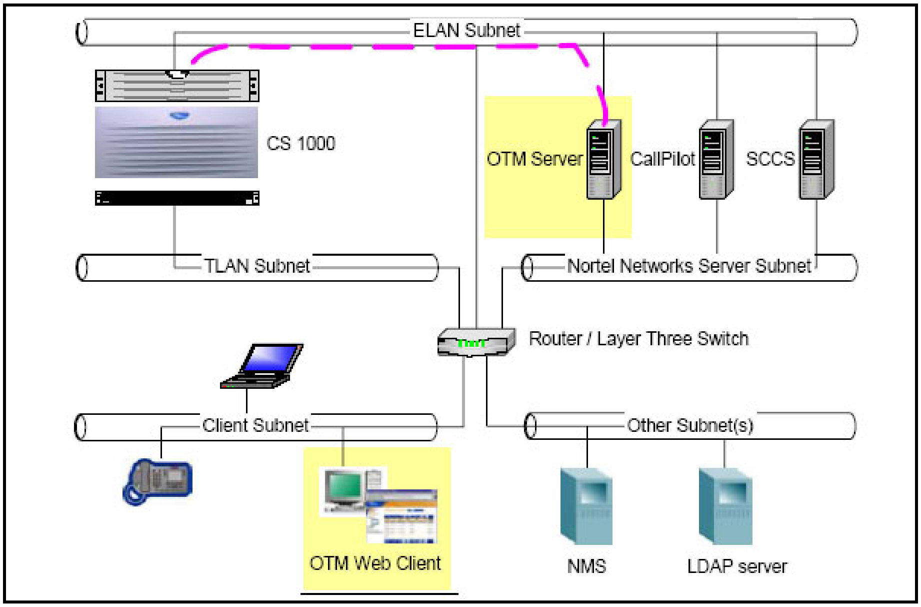
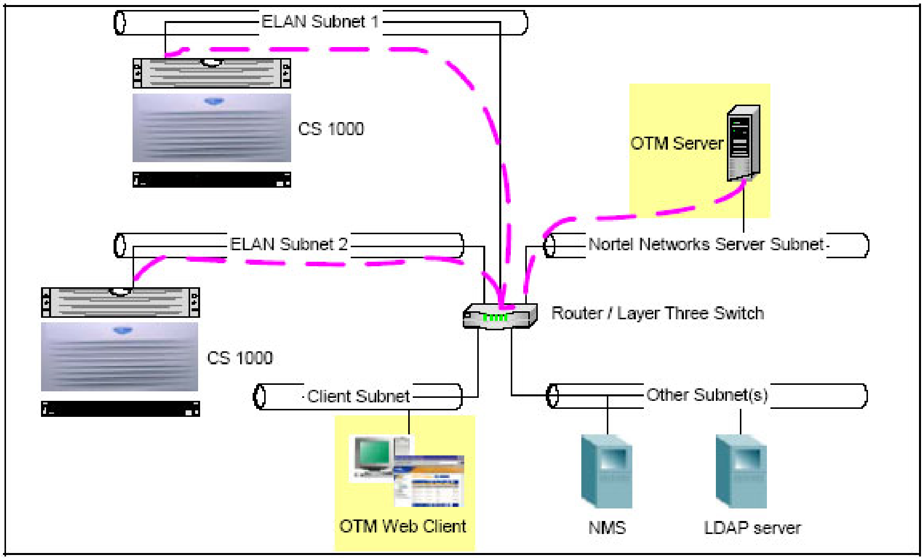


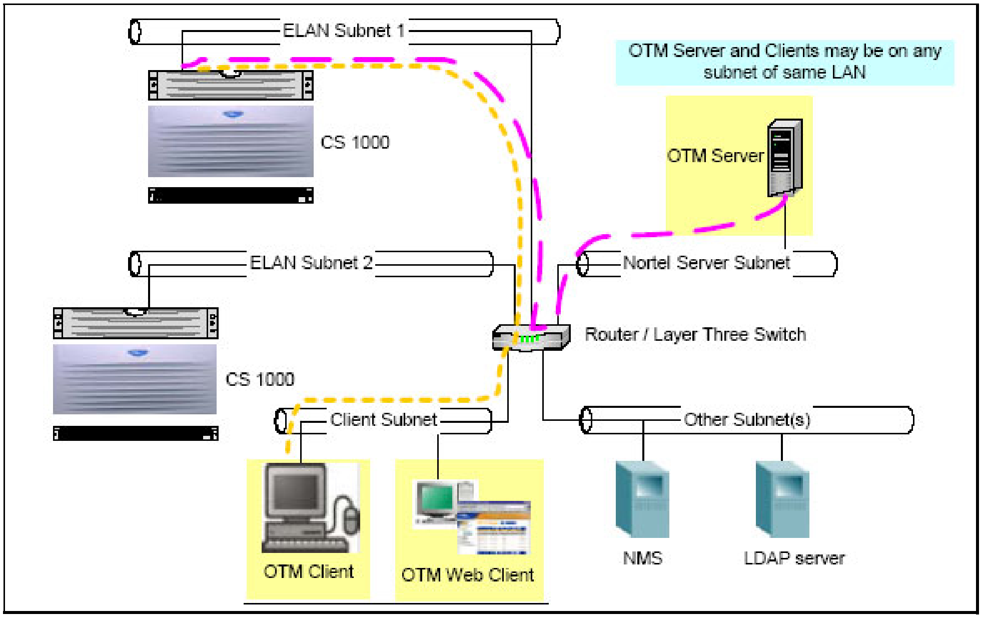
Figure 147
Standalone OTM server with routed connections



OTM server with OTM clients

In this configuration the OTM server is connected to a number of OTM clients, all on the same LAN (due to bandwidth and other restrictions). There may be optional web clients. Here, routed connections are used from the OTM server/clients to the ELAN subnets of managed systems (via the Nortel server subnet). Figure 148 illustrates this configuration.

Figure 148
OTM server with OTM clients



Since OTM clients cannot be connected to the OTM server across a WAN, to get full GUI capabilities across a WAN, Nortel recommends that pcAnywhere be used to connect to the OTM server and/or OTM clients.

VPN connections

OTM does not have any special support for Virtual Private Network (VPN) connections. It is possible for OTM to use a VPN connection as long as this is transparent to the OTM application. One example would be for a remote user to use the OTM web client using a VPN connection over the Internet into the customer Enterprise IP network to access the OTM server.

Bandwidth utilization

The trade-off is the cost of OTM versus the cost of increased network bandwidth or network subnets. Once OTM servers are attached to the WAN, the customer’s network may be impacted, but there is a saving on the number of OTMs needed.

Never expect to fully utilize Ethernet bandwidth. Performance degrades quickly as the utilization exceeds a certain threshold (approximately 35 percent). Consult the network administrator for details on network bandwidth utilization.

Table 18 lists the average and peak traffic for the ELAN subnet and Nortel server subnet. This is based upon traffic analysis of a system running on a CP4 CPU. For an Cabinet system system, divide the ELAN subnet numbers by 2, except for alarms. For the CPP CPU, multiply the ELAN subnet numbers by 4, except for alarms.

Table 18
Network bandwidth usage per system

	Transfer rate (bits/second)	
OTM Activity	**Average**	**Peak**
Station Add/Chg/Del, ELAN subnet	32 kb	32 kb
Station Sync with M1, ELAN subnet	NA	48 kb
CDR, ELAN subnet	35 kb	70 kb
Traffic, ELAN subnet	24 kb	48 kb
Alarm, ELAN subnet	1 kb	3 kb
Sync with LDAP server, Nortel server subnet	NA	720 kb
Total, ELAN subnet	~92 kb	~201 kb
Total, Nortel server subnet		~720 kb

Alarm Processing

There are OTM alarms and IP Line managed system alarms.

OTM alarm details

The OTM Trap server can handle 25–50 incoming SNMP traps per second. However, this limitation varies considerably with network load, PC processing power, and CPU availability.

Traps are stored in a circular queue of 1360 traps. You can view the queue using the web Alarm Browser. If the rate of trap arrival is heavy, some traps are not entered into the queue even though they are received by the Trap server and Alarm Notification application. The circular queue can handle an incoming rate of 50 traps in 10 seconds without any loss of information.

An SNMP trap has an average size of approximately 400 bytes. You can use this information to approximate the bandwidth requirements for trap processing. For example, 1000 devices, each producing one trap every 10 seconds, would require a bandwidth of 320 Kbps:

400 bytes/trap * 8 bits/byte * 1000 devices * 0.1 trap/sec/device = 320 Kbps

IP Line/IP Trunk /Switch alarm details

Under normal conditions, a system generates one trap approximately every ten seconds. Beginning with X11 Release 25, you can use filtering on the system to reduce the output of traps. However, there is no filtering capability on IP Line/IP Trunk. IP Line/IP Trunk does not generate traps under normal operating conditions. In an abnormal situation, IP Line/IP Trunk could be expected to generate an alarm every 5 seconds.

IP Line/ IP Trunk may generate a large number of alarms when Quality of Service (QoS) monitoring is enabled. When QoS monitoring is enabled, an alarm is raised or cleared for every QoS threshold crossing (excellent, good, or fair) per codec. A network with varying QoS has many threshold crossings resulting in a large number of alarms.

Recommended usage

For bandwidth and processing reasons, alarm traffic should be minimized. If alarms from the switch are sent to OTM, use filtering to limit the traffic to only important alarms. Since it is unlikely that multiple Voice Gateway Media cards will simultaneously exhibit problems, the alarms generated by Voice Gateway Media cards should not create traffic problems. To limit alarm traffic, Nortel recommends that you not enable Network QoS Monitoring. Changes to IPLine/IP Trunk to allow filtering helps this situation. The incoming rate of alarms must match the handling capabilities of the OTM configuration.

The alarm circular queue can be quickly exhausted if there is significant alarm traffic.

Operational measurement processing

Voice Gateway Media cards collect operational measurement (OM) information on an hourly basis. This data is stored on the cards until it is retrieved by OTM using an FTP operation. The data can be retrieved on demand, however, the FTP operation is normally scheduled to occur on a daily basis. The data file generated by an Voice Gateway Media card in a 24-hour period is approximately 5 KB.

When retrieval occurs, the information is collected from all cards on all nodes. There is no capability to retrieve the information on an individual node basis.

The retrieved information is parsed and written to comma separated values (CSV) files on the OTM server. The number of files created is dependent upon the number of records retrieved.

If there are many cards in the system, the retrieval operation should be scheduled to occur during off-hours.

OTM system performance

Network impact on OTM Windows client/server

As mentioned in "OTM server and client's overview" on page 71, the OTM Windows clients do not operate in a typical client-server mode. All data is stored on the OTM server and accessed by the OTM client.

The network performance has a significant impact on OTM Windows client/server applications. In particular, the applications are sensitive to the RTT and bandwidth. The RTT is important since numerous smaller packets of data are sent between the server and the client. Very high bandwidth is consumed since Microsoft Access database accesses by the client require transfer of the entire databases. If the RTT or bandwidth is limited, it will result in performance degradation. This is manifested by slow response times, and if sufficiently poor may result in failure of operations (e.g., timeouts).

The demands on the network are illustrated below for the scenario of a login to OTM from the client, followed by opening up Station Administration. The measurements were done in a lab environment with a dedicated LAN connection. Performance in the customer environment varies depending on network utilization and system size (for example, number of lines, number of managed systems). During this operation over 2MB of data was transferred, and over 7000 packets were transferred between the OTM server and the OTM client. Subsequent operations would result in substantially smaller data transfers. Similar data transfers would take place for other operations, such as TBS reporting.

The impact of the high bandwidth consumption on other customer network applications should be considered when deploying OTM clients on the customer enterprise IP network.

Figure 149 on page 310 shows the relationship between Station Administration response time and RTT in a lab environment.

Figure 149
Station Administration Response Time versus Round Trip Time

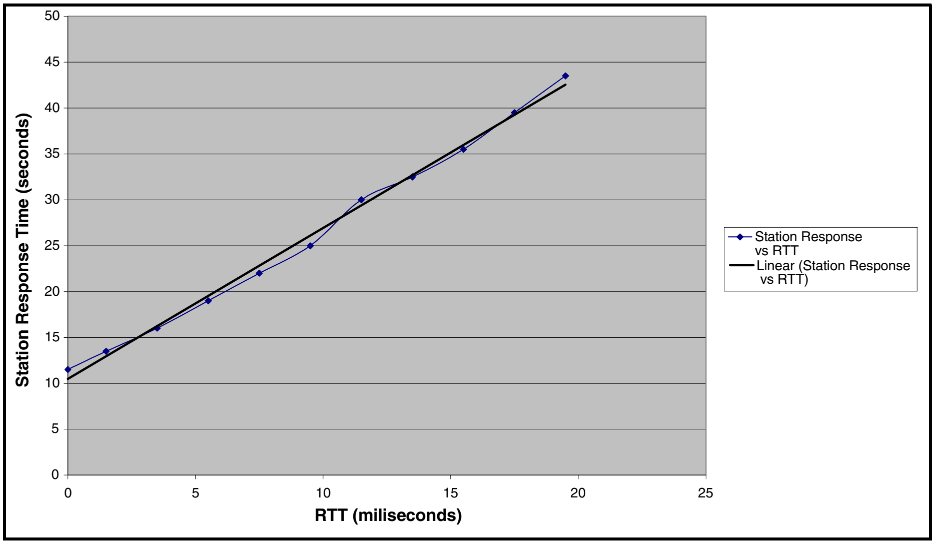
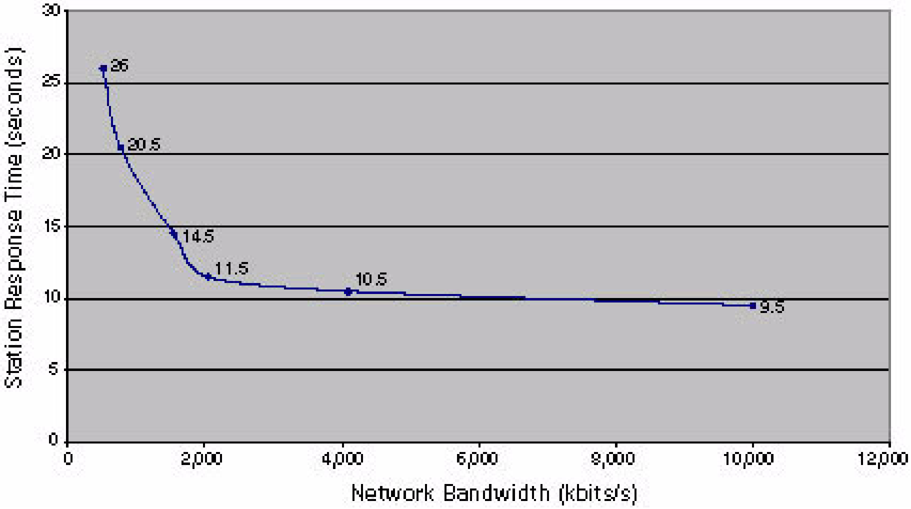


Figure 150 shows the relationship between Station Administration response time and Bandwidth in a lab environment. Note the negative exponential impact of using bandwidth that is less than 2 Mbps.

Figure 150
Station Administration Response Time versus Network Bandwidth



Hostname resolution

LMHOSTS file

When Microsoft TCP/IP is used on a local network with any combination of computers running Windows 2000, Windows XP, and so on, server names are automatically matched to their corresponding IP addresses. However, to match server names across remote networks connected by routers (or gateways), the LMHOSTS file can be used if WINS servers are not available on the network. Figure 151 on page 312 and Figure 152 on page 313 show an example of an LMHOSTS file.

The LMHOSTS file is commonly used to locate remote computers for Microsoft networking file, printer, and remote access services, and for domain services such as logon, browsing, replication, and so on.

Microsoft TCP/IP loads the LMHOSTS file into memory when the computer is started. The LMHOSTS file is a text file in the Windows directory that lists the IP addresses and computer names of remote Windows networking servers with which you want to communicate. The LMHOSTS file should list all the names and IP addresses of the servers you regularly access.

For example, the LMHOSTS table file entry for a computer with an address of 192.53.63.2 and a NetBIOS computer name of Building1 would be:

192.53.63.2 Building1

Procedure 68
Creating an LMHOSTS file

To create an LMHOSTS file:

1 Use a text editor to create a file named LMHOSTS.

Or

Edit the default file named LMHOSTS.SAM.

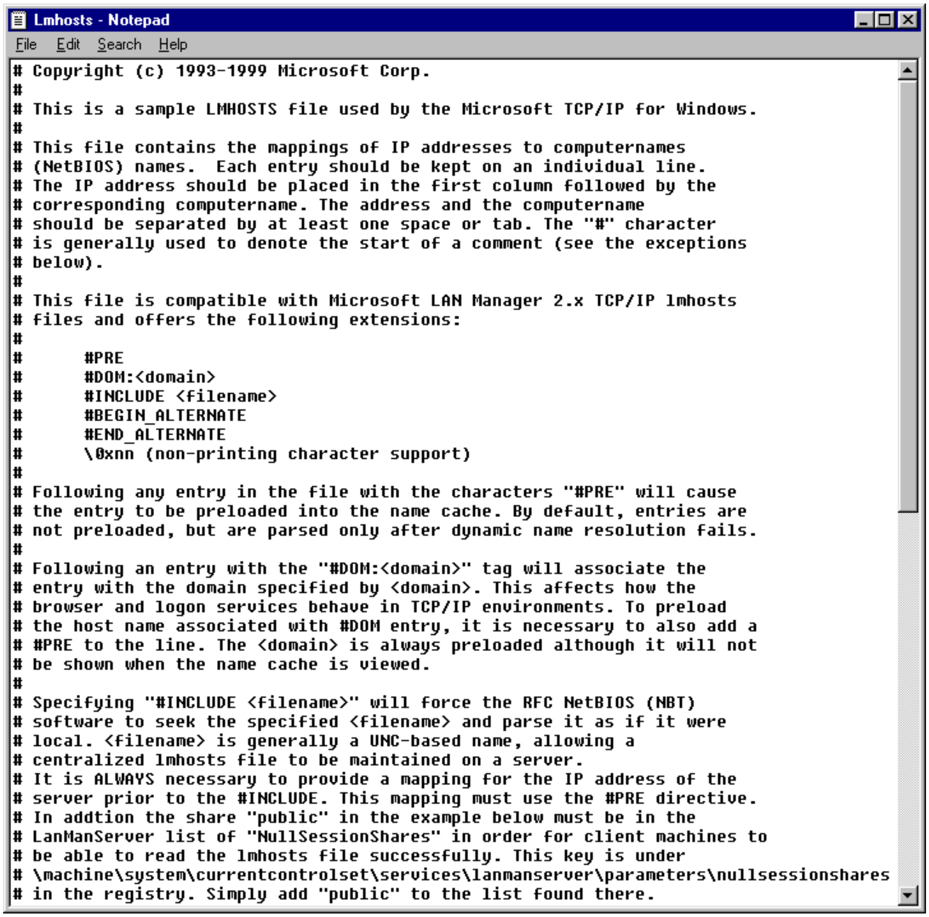
This file is located in the ***<system root>***\system 32\drivers\etc directory for Windows 2000 and Windows XP systems.

2 In the LMHOSTS file, type the IP address and the host name of each computer that you want to communicate with.

For example, on each OTM client machine add the OTM server name and its IP address. Separate the items with at least one space.

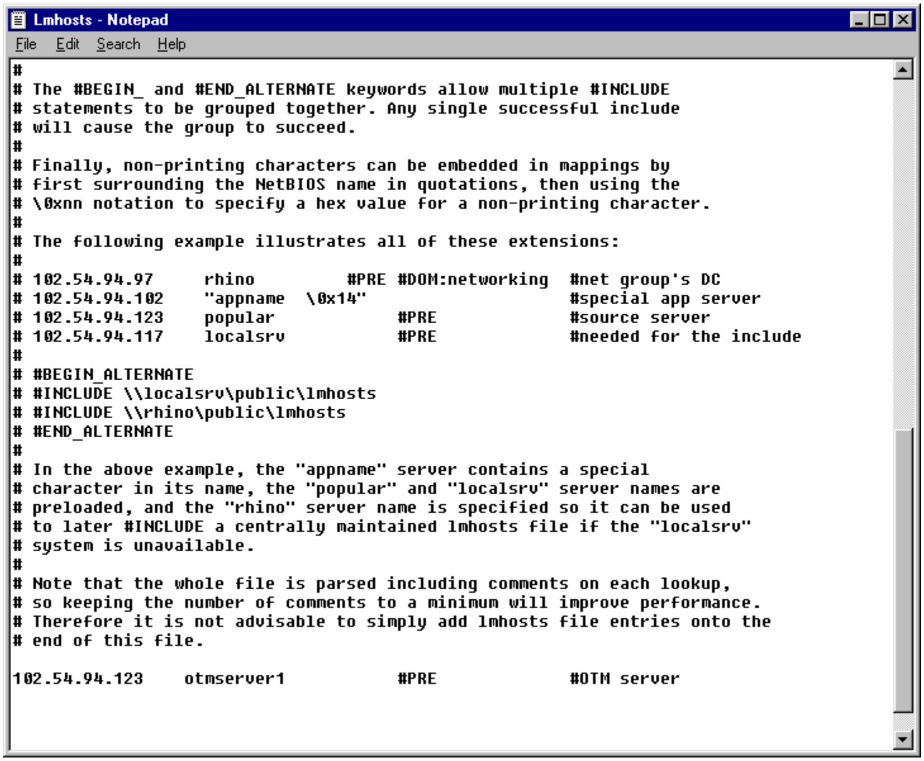
Note that entries in the LMHOSTS file are not case-sensitive.

Figure 151
Example of LMHOSTS file (part 1)



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names.  Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lmhosts
# files and offers the following extensions:
#
#      #PRE
#      #DOM:<domain>
#      #INCLUDE <filename>
#      #BEGIN_ALTERNATE
#      #END_ALTERNATE
#      \0xnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RFC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
# In addtion the share "public" in the example below must be in the
# LanManServer list of "NullSessionShares" in order for client machines to
# be able to read the lmhosts file successfully. This key is under
# \machine\system\currentcontrolset\services\lanmanserver\parameters\nullsessionshares
# in the registry. Simply add "public" to the list found there.
```

Figure 152
Example of LMHOSTS file (part2)



```
#
# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE
# statements to be grouped together. Any single successful include
# will cause the group to succeed.
#
# Finally, non-printing characters can be embedded in mappings by
# first surrounding the NetBIOS name in quotations, then using the
# \0xnn notation to specify a hex value for a non-printing character.
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97     rhino         #PRE #DOM:networking  #net group's DC
# 102.54.94.102    "appname  \0x14"                    #special app server
# 102.54.94.123    popular            #PRE             #source server
# 102.54.94.117    localsrv           #PRE             #needed for the include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
#
# In the above example, the "appname" server contains a special
# character in its name, the "popular" and "localsrv" server names are
# preloaded, and the "rhino" server name is specified so it can be used
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
# end of this file.

102.54.94.123    otmserver1           #PRE             #OTM server
```

3 Save the file as LMHOSTS.

Note: The filename is LMHOSTS with no extension.

End of Procedure

LMHOSTS is normally used for smaller networks or to find hosts on remote networks that are not part of the WINS database (because name query requests are not broadcast beyond the local subnetwork). If WINS servers are in place on an internetwork, users do not have to rely on broadcast queries for name resolution because WINS is the preferred method for name resolution. Therefore, with WINS servers in place, LMHOSTS may not be necessary.

The LMHOSTS file is read when WINS or broadcast name resolution fails. Resolved entries are stored in a system cache for later access. When the computer uses the replicator service, and does not use WINS, LMHOSTS entries are required on import and export servers for any computers on different subnetworks participating in the replication.

Procedure 69
Configuring TCP/IP to use LMHOSTS

To configure TCP/IP to use LMHOSTS on a Windows PC:

1. Open Network and Dial-up Connections.
2. Right-click the network connection you want to configure, and then click **Properties.**
3. On the General tab (for local area connection) or the Networking tab (all other connection), click Internet Protocol (TCP/IP), and then click **Properties**. Click **Advanced**, click the WINS tab. Select the Enable LMHOSTS lookup check box. This option is selected by default.
4. To specify the location of the file that you want to import into the LMHOSTS file, click Import LMHOSTS, and then select the file in the Open dialog box.
5. To complete the configuration, either:

   a. Reboot the computer

   Or

   b. Go to the command prompt, and enter the following text:

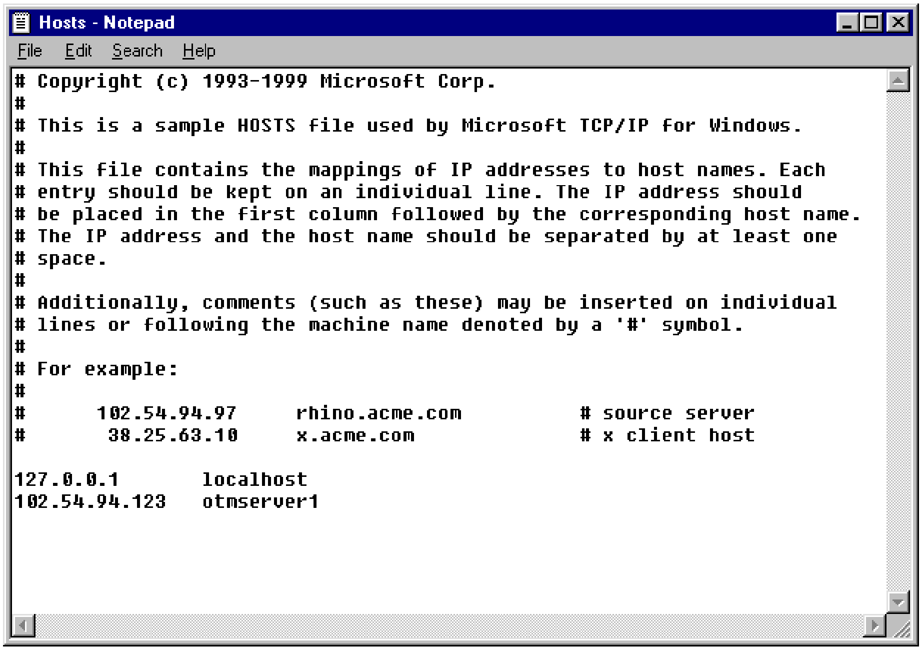
```
nbstat -R
nbstat -c
```

End of Procedure

HOSTS file

The HOSTS file contains a list of host name to IP address mappings. It is a regular text file. The HOSTS file is located in the ***<system root>***\system 32\drivers\etc directory for Windows XP and Windows 2000 systems. See Figure 153 on page 315.

Figure 153
Sample HOSTS file



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
102.54.94.123   otmserver1
```

Use a text editor to edit the HOSTS file. In the HOSTS file, type the IP address and the host name of each computer with which you want to communicate, for example, on each OTM client computer add the OTM server IP address followed by its name. Separate the items with at least one space. Entries in the HOSTS file are not case-sensitive. Note that the HOSTS filename has no extension.

End of Procedure

Asset Limits on Employee Editor

The number of telephones assigned to an employee has significant impact on the performance of Employee Editor.

Figure 154 on page 316 shows the relationship between the number of telephones assigned to an employee and the time taken by Employee Editor to load/modify the details of a particular employee.

Figure 154
Telephones assigned to a single employee

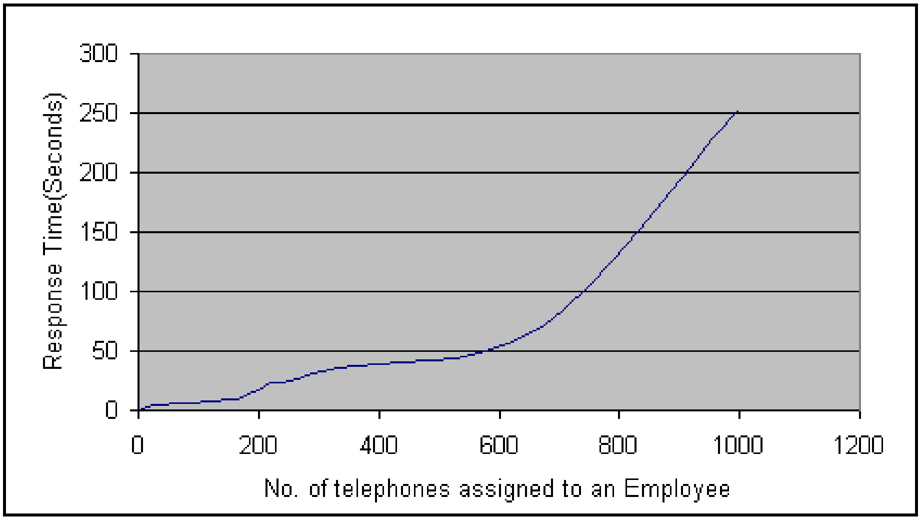


Figure 154 shows the performance of Employee Editor in a lab environment. Customers may experience different response times depending on their system configuration.

This trend in performance is due to the large number of entries to be processed and the fact that the operations are memory-intensive. As the number of entries increases, system performance worsens, and the system could run out of virtual memory.

OTM port usage

When using OTM to monitor and maintain systems, various ports and protocols are used to communicate between OTM and the desired client, server, or application. Table 19 on page 317 lists typical port usage based on the flow of information between OTM and these system components.

Table 19
OTM Port Usage (Part 1 of 2)

OTM Sending To	Port	Type	Protocol	Component	Remarks
Meridian 1 or Communication server 1000 system	513	TCP	Rlogin	Session Connect, System Terminal, Station Admin, CPND, List manager, ESN.	Using netstat
Meridian 1 or Communication server 1000 system	161	UDP	SNMP	Alarm Management, Maintenance Window	Microsoft Default Port
Meridian 1 or Communication server 1000 system	21	TCP	FTP	Corporate Directory & DBA	Microsoft Default Port
Meridian 1 or Communication server 1000 system	20	TCP	FTP	Corporate Directory & DBA	Microsoft Default Port FTP -data
SMTP server	25	TCP	SMTP	Alarm Notification	Microsoft Default Port
IP Line/IP Trunk	21	TCP	FTP	OTM	Microsoft Default Port
Win client	139	TCP	NetBEUI	Windows client File Sharing	Microsoft Default Port
LDAP server	389	TCP	LDAP	LDAP Synchronization	Microsoft Default Port
LDAP server Over SSL	636	TCP		LDAP synchronization	Microsoft Default Port (LDAP SSL)
OTMReceiving From	**Port**	**Type**	**Protocol**	**Component**	**Remarks**
web client	80	TCP	HTTP	web CS, Desktop Services, web telecom billing system	Microsoft Default Port

Table 19
OTM Port Usage (Part 2 of 2)

OTM Sending To	Port	Type	Protocol	Component	Remarks
web client	4789-5045	TCP		Virtual System Terminal Note:- VT uses 1 port per session. Start with 4789.	The base port can be changed from 4789.
Win client	139	TCP	NetBEUI	Windows client File Sharing	Microsoft Default Port
Win client	135	TCP/ UDP		Login	RPC, SCM used by DCOM
Win client	1583	TCP	Btrieve/ Pervasive	Station Administration	Refer to Pervasive documentation.
Win client	3351	TCP	Btrieve/ Pervasive	Station Administration, Note uses 1 port per session. Start from 3351	Refer to Pervasive documentation.
Meridian 1 or Communication server 1000 sending to	**Port**	**Type**	**Protocol**	**Component**	**Remarks**
OTM	162	UDP	SNMP	Alarm Traps(LD 117), Maintenance window	Microsoft Default Port
OTM	1929 2058	UDP		DBA Note: 1 port per session. Start from 1929 till 2057. 2058 and onward is used as Data ports till 2185.	
DECT	5099	TCP	RMI	OTMDECT	Using netstat command

Sample walk-through of computations

This section provides a sample walk-through of computations used to determine how many systems and OTM clients can be connected to an OTM server. Factors involved include:

- Type of OTM feature configuration
- Type of OTM server and system hardware
- Constraints on CPU usage and off-hours work

Sample configurations based on application usage and features

The following are the sample configurations based upon application usage and features that impact server resources. These configurations do not reflect how OTM is packaged (for example, General, Enhanced, and Premium).

Example 1

Configuration, Station, IP Line/IP Trunk , Maintenance Windows, Alarm Management, DECT configuration, and other applications

Example 2

Configuration and Alarm Management with web/OTM client Access and LDAP Service and web Station Write configured for end users (full OTM system)

Example 3

Alarm Management, Data Buffering & Access (DBA), Traffic Analysis, OTM as a Buffer Box replacement (Access server)

Sample PC and system configurations

The following are the PC and system configurations used for this example:

- OTM server and OTM clients connected to a 100 MB network, utilizing no more than 35 percent of its bandwidth

  Refer to Figure 146 on page 305.

- 512 MB of physical memory
- ATAPI Hard Disk
- 2 OTM Windows and/or web clients active at the same time at peak usage
- Cabinet system averaging 400 lines per system

  - Averaging 1 call records/second generated (peak is 6)
- CS 1000M MG and Meridian 1 PBX 81C with CP4 averaging 2000 lines per system
  - Averaging 3 call records/second generated (peak is 32)

Operational constraints

The following are the operational constraints:

- During normal operation, do not use more than 80% of the CPU for routine operations to leave time to perform other operations. For example, Maintenance windows and IP Line/IP Trunk configuration.
  Routine operations as defined in Table 17 on page A-296 are:
  - Station Add/Move/Change from server
  - Station Add/Move/Change from OTM client
  - Station web access
  - web Desktop Services Write capability for End Users
  - Alarms monitoring
  - CDR and Traffic Collection
- Normal operations are performed daily during normal working hours (for example, from 8:00 a.m. to 5:00 p.m. every day). The default value is the peak six hours of the day (9:00 a.m. to 12:00 p.m. and 1:00 p.m. to 4:00 p.m.). Daily activities are based on the following assumptions:
  - Percentage of lines changed by the network administrator per day is 1 percent. For example, a system with 2000 lines has 20 lines changes by the network administrator during a normal work day.
  - Number of lines changed by end users through web Desktop Services is 0.25 percent. For example, a system with 2000 lines has approximately 5 lines changed by end users during a normal work day provided that the web Desktop Services Write feature is configured.
- Off-hours operations can use 100 percent of the CPU, and are limited as follows (from Table 17):
  - Station retrieve/reconcile is performed once a week, or twice a month, on the weekend. The maximum period of time reserved for this activity is theoretically 48 hours. For these examples, reserve the time from 9:00 p.m. on Sunday to 6:00 a.m. on Monday, or 9 hours.

- — Station transmit is scheduled and performed during the peak 6 hours (for example, from 9:00 a.m. to 12:00 p.m. and 1:00 p.m. to 4:00 p.m.).
- — Assume, for a Cabinet system, that OTM can run Station update for two devices simultaneously (based upon processor speed and CPU usage figures).
- — CDR Reports are performed once a day. For these examples, off-hours are from 12:00 a.m. (midnight) to 6:00 a.m., or 6 hours.
- — LDAP Sync is performed once a week, on the weekend.
  For these examples, reserve the time from 9:00 p.m. Sunday to 6:00 a.m. on Monday, or 9 hours.

Table 20 and Table 21 provide OTM capacity estimates, based upon the information provided in the succeeding sections, and using the configuration examples previously defined. In the numbers presented, the most limiting factor from routine operation, off-hours operation, and network bandwidth is entered into the tables. The numbers in these tables were calculated as follows:

Table 20
Maximum configuration for an Meridian 1 PBX 81 network averaging 2000 lines per system

Configuration example	Number of systems	Number of lines	Number of OTM clients
1	5	10 800	
2	5	10 800	
3	3	6 480	20
4	2	4 400	

Table 21
Maximum configuration for a Meridian 1 PBX 11C Cabinet or CS 1000 network averaging 400 lines per system

Configuration example	Number of Meridian 1 or CS 1000 systems	Number of lines *	Number of simultaneous OTM clients
1	26	10 800	
2	26	10 800	
3	26	10 800	20
4	6	2 600	
* Assumes two simultaneous systems.			

Configuration calculations

Example: Meridian 1 PBX 81 = 5 Meridian 1 systems or 10,800 lines

- Routine operation:
  - If administration is done primarily through the OTM Windows interface: Adds/Moves/Changes = approximately 23.8% CPU utilization
  - If administration is done primarily through the OTM web interface: Adds/Moves/Changes = approximately 27% CPU utilization
- Off-hours operation:
  - Station update = 1 record/3 seconds
  - 9 hours = 32,400 seconds
  - 32,400 seconds * 1 record/3 seconds = 10,800 records (lines)
  - 10,800 lines/2000 lines per system = approximately 5 Meridian 1 systems
- Network bandwidth:
  - Station (peak) operations = 80 kb/second
  - Network = 100 MB/second
  - % usage per system = 80 kb/second / 100 MB/second = approximately 0.1%
  - 35% allowed usage / 0.1% per system = approximately 350 Meridian 1 systems

Example: Meridian 1 PBX 11C Cabinet = 26 Meridian 1 or Communication server 1000 systems or 10,800 lines:

- Routine operation:
  - If administration is done primarily through the OTM Windows interface: Adds/Moves/Changes = approximately 23.8% CPU utilization
  - If administration is done primarily through the OTM web interface: Adds/Moves/Changes = approximately 27% CPU utilization
- Off-hours operation:
  - Station update = 1 record/6 seconds
  - 9 hours = 32,400 seconds
  - 32,400 seconds * 1 record/6 seconds = 5,400 records (lines)
  - 5,400 lines/400 lines per system * 2 simultaneous systems = approximately 26 Meridian 1 or Communication server 1000 systems

- Network bandwidth:
  - Station (peak) operations = 40 kb/second
  - Network = 100 MB/second
  - % usage per system = 40 kb/second / 100 MB/second = approximately 0.05%
  - 35% allowed usage / 0.05% per system = approximately 700 Meridian 1 or Communication server 1000 systems

The average alarms and DECT usage are so small that their impact on routine, off-hour, and network bandwidth is negligible.

Example: Meridian 1 PBX 81 = 3 Meridian 1 systems or 6,480 lines

- Routine operation:
  - If administration is done primarily through the OTM Windows interface, then Adds/Moves/Changes = approximately 14.28% CPU utilization
  - If administration is done primarily through the OTM web interface, then Adds/Moves/Changes = approximately 16.2% CPU utilization
  - OTM client usage on OTM server = approximately 4% per client
    80% CPU time / 4% per client = 20 OTM clients
- Off-hours operation:
  - Station update = 1 record/3 seconds
  - OTM client station update = 1 record/5 seconds
  - LDAP Sync operation = 10 records/second
    For 100,000 records = approximately 2.8 hours
  - 9 hours = 32,400 seconds
  - 32,400 seconds * 1 record/3 seconds = 6,480 records (lines)
  - 6,480 lines / 2000 lines per system =approximately 3 Meridian 1 systems
- Network bandwidth:
  - Station (peak) operations = 80 kb/second
  - LDAP Sync operation = 720 kb/second
    Percent usage of network = approximately 0.7%
  - Network = 100 MB/second
  - Percent usage per system = 80 kb/second / 100 MB/second = approximately 0.1%

  - 35% allowed usage / 0.1% per system = approximately 350 Meridian 1 systems

Example: Meridian 1 PBX 81= 2 Meridian 1 systems or 4,400 lines

- Routine Operation:
  - CDR plus traffic = approximately 3.5% per system
  - If administration is done primarily through the OTM Windows interface:

    Adds/Moves/Changes = approximately 9.7% CPU utilization
  - If administration is done primarily through the OTM web interface:

    Adds/Moves/Changes = approximately 11% CPU utilization
- Off-hours operation:
  - Parsing plus Cost Report = 20 records/second
  - 18 hours of call collection operation = 64,800 seconds
  - 64,800 seconds * 3 call records/second/system = 194,400 call records per system
  - 6 hours of report generation = 21,600 seconds
  - 21,600 seconds * 20 records/second = 432,000 call records in 6 hours
  - 432,000 call records/194,400 call records per system = approximately 2 Meridian 1 systems
- Network bandwidth:
  - CDR plus traffic (peak) operations = 118 kb/second
  - Network = 100 MB/second
  - Percent usage per system = 118 kb/second / 100 MB/second = approximately 0.1%
  - 35% allowed usage / 0.1% per system = approximately 350 Meridian 1 systems

Example: Meridian 1 PBX 11C Cabinet = 6 Meridian 1 or Communication server 1000 systems or 2,600 lines

- Routine operation:
  - If administration is done primarily through the OTM Windows interface:

    Adds/Moves/Changes = approximately 5.73% CPU utilization
  - If administration is done primarily through the OTM web interface:

    Adds/Moves/Changes = approximately 6.5% CPU utilization
- Off-hours operation:
  - Parsing plus Cost Report = 20 records/second
  - 18 hours of call collection operation = 64,800 seconds
  - 64,800 seconds * 1 call record/second/system = 64,800 call records per system
  - 6 hours of report generation = 21,600 seconds
  - 21,600 seconds * 20 records/second = 432,000 call records in 6 hours
  - 432,000 call records at 64,800 call records/system = approximately 6 Meridian 1 or Communication server 1000 systems
- Network bandwidth:
  - CDR plus traffic (peak) operations = 59 kb/second
  - Network = 100 MB/second
  - Percent usage per system = 59 kb/second / 100 MB/second = approximately 0.05%
  - 35% allowed usage / 0.05% per system = approximately 700 Meridian 1 or Communication server 1000 systems

OTM language support

OTM supports the following language configurations:

2.2 OTM Languages supported for English and Regional OS								
client language locale should be set to the language in which OTM is to be run								
server OS & Locale	client Regional OS							
	English		Japanese	Simplified Chinese	Portuguese	Spanish	French	German
	WinXP Pro	Win2K Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/XP Pro	Win2K/ XP Pro	Win2K/ XP Pro	Win2K/ XP Pro
English Win2K server (English Locale)	English OTM	English OTM			English OTM	English OTM	English OTM	English OTM
English Win2K server (French Locale)							French OTM	
English Win2K server (German Locale)								German OTM
Japanese Win2K server			English OTM					
Simplified Chinese Win2K server				English OTM				
Standalone machine (no OTM client)	English OTM	English OTM	English OTM	English OTM	English OTM	English OTM	English or French OTM	English or German OTM

Appendix B: Installation checklist

Contents

This appendix contains information on the following topics:

Overview

Use the following quick reference as a checklist or reminder when starting a new OTM installation.

Installation requirements

Software and memory

[ ] Required X11 packages (296, 315, and 351 depending on applications being installed)

[ ] Minimum of 48 MB of memory on the switch

Ethernet connections

[ ] X11 Release 22 or later

[ ] Release 24B or later for Data Buffering and Access

[ ] IOP, IOP/CMDU, or IODU/C cards for Meridian 1 PBX 51C, 61C, 81, or 81C

[ ] Ethernet AUI cables to be attached to each IOP (Meridian 1 PBX 51C, 61C, 81, or 81C)

[ ] NTDK27 Ethernet cable for Meridian 1 PBX 11C Cabinet

[ ] Transceivers to connect to the LAN

[ ] Router

PPP connections

[ ] Hayes-compatible modem

[ ] SDI port available on the system (configured for SCH only)

[ ] Serial cable to connect the modem to the SDI port

Serial connections

[ ] SDI port available on the switch (configured for SCH only)

[ ] Hayes-compatible modem for remote connection (optional)

[ ] Serial cable to connect the modem to the SDI port

Programming the switch

[ ] Enable Name Option in LD 17.

[ ] Define Limited Access Password in LD 17.

[ ] For Serial communication: Configure a TTY with User = SCH in LD 17.

[ ] For Ethernet or PPP communication: Configure a pseudo TTY (PTY) with User = SCH MTC BUG in LD 17.

[ ] Configure Ethernet at the switch in LD 117.

[ ] Define the Gateway (router) IP address on the switch in LD 117.

[ ] Configure PPP at the switch in LD 117.

[ ] INIT the switch.

[ ] Enable the new IP address (defined in LD 117) in LD 137.

[ ] Enable Database Disaster Recovery (DDR) in LD 117.

[ ] Set open alarm destination in LD 117.

[ ] Set up Data Buffering and Access in LD 117.

[ ] Set up filtering in the system to filter out information and minor messages.

PC/server installation requirements

Single (stand-alone) OTM installation

Stand-alone mode consists of a single web-based client and no Windows clients.

[ ] Intel Pentium III Processor 600 MHz

[ ] 2 GB (1 GB plus customer data storage)

[ ] 512 MB of RAM recommended

[ ] One or two Ethernet Network Interface Cards (if applicable)

[ ] Windows XP Professional (Service Pack 2), Windows 2000 server (Service Pack 4), Windows 2000 Professional (Service Pack 4)

[ ] OTM dongle/USB dongle

[ ] Printer port (LPT)/USB Port required for dongle

[ ] OTM CD and keycode

[ ] Remote Access Service (RAS)

[ ] Modem(s) for remote access (optional)

If multiple web clients are connected to the stand-alone system, the requirements are equivalent to the OTM server requirements.

OTM server installation

[ ] Intel Pentium III Processor 600 MHz

[ ] 3 GB hard drive (1 GB of free space plus customer data storage requirements)

[ ] 512 MB of RAM recommended

[ ] One or two Ethernet Network Interface Cards (if applicable)

[ ] PC COM port with 16550 UART

[ ] Hayes compatible modem (optional)

[ ] Windows 2000 server (Service Pack 4)

[ ] Remote Access Service (RAS)

[ ] OTM dongle/USB dongle

[ ] OTM CD and Keycode

[ ] Configure and test network interfaces

[ ] Enable IP routing (if applicable)

OTM client installation

[ ] Windows client - Pentium III 400 MHz (Pentium III 600 MHz recommended)

[ ] 2 GB hard drive with 500 MB of free space

[ ] Windows client - 256 MB of RAM minimum (512 MB of RAM recommended) web client - 256 MB of RAM

[ ] Windows client - PC COM port with 16550 UART

[ ] One or two Ethernet Network Interface Cards (if applicable)

[ ] Windows XP Professional (Service Pack 2) and Windows 2000 Professional (Service Pack 4)

[ ] Windows client - Remote Access Service (RAS)

[ ] Windows client - OTM CD and Keycode (no Dongle required)

[ ] Web client - Java Runtime Environment (JRE) 1.4.2, and Microsoft Internet 6.0 SP 1 or Netscape Navigator 4.79

Index

Nortel Communication Server 1000

Optivity Telephony Manager

Installation and Configuration

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Publication number: 553-3001-230
Document release: Standard 3.00
Date: August 2005
Produced in Canada